**ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**
**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ**

**КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ**

# КВАЛІФІКАЦІЙНА РОБОТА

на тему:

**«Підвищення можливостей виявлення загроз корпоративній інформаційній системі на прикладі QRadar Use Case Manager**

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека
*(код, найменування спеціальності)*
освітньо-професійної програми Інформаційна та кібернетична безпека
*(назва)*

*Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело*
_____ Артем КОВРИЖКО

Виконав: здобувач(ка) вищої освіти групи БСДМ-61
КОВРИЖКО АРТЕМ
(ПРІЗВИЩЕ, Ім'я)

Керівник: СОБЧУК Андрій
*д.т.н, професор* (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
*д.т.н., професор* (ПРІЗВИЩЕ, Ім'я)

Київ 2024

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**
**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ**

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

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
“___”_____ 2023 року

# З А В Д А Н Н Я
## НА КВАЛІФІКАЦІЙНУ РОБОТУ

Коврижку Артему Олександровичу
(прізвище, ім’я, по батькові)

1. Тема кваліфікаційної роботи:
«Підвищення можливостей виявлення загроз корпоративній інформаційній системі на прикладі QRadar Use Case Manager»
керівник кваліфікаційної роботи: Собчук Андрій, д.ф., доцент,
*(ПРІЗВИЩЕ, Ім’я, науковий ступінь, вчене звання)*
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «19» жовтня 2023р. №145.

2. Строк подання студентом кваліфікаційної роботи: 15.12.2023 р.

3. Вихідні дані до кваліфікаційної роботи:
інформаційна система організації;
QRadar Use Case Manager;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз необхідності виявлення загроз корпоративній інформаційній системі.
2. Методи та засоби виявлення загроз корпоративній інформаційній системі.
3. Розроблення варіанта системи протидії та виявлення загроз базі рішення QRadar Use Case Manager.

5. Перелік ілюстративного матеріалу:
Презентація PowerPoint

6. Дата видачі завдання 19.10.2023 р.

## КАЛЕНДАРНИЙ ПЛАН

| № зп | Назва етапів кваліфікаційної роботи | Строк виконання етапів роботи | Примітка |
|---|---|---|---|
| 1. | Визначення актуальності проблеми можливостей виявлення загроз корпоративній інформаційній системі. | 19.10.2023 р. | |
| 2. | Аналіз наукової та технічної літератури за темою кваліфікаційної роботи. | 22.10.2023 р. | |
| 3. | Аналіз методів та засобів для виявлення загроз корпоративній інформаційній системі. | 27.10. 2023р. | |
| 4. | Розроблення варіанта системи виявлення загроз корпоративній інформаційній системі на базі рішення QRadar Use Case Manager. | 03.11.2023 р. | |
| 5. | Розроблення власної SIEM з Use Case для виявлення та протидії загрозам | 15.11.2023 р. | |
| 6. | Оформлення результатів дослідження. Проходження плагіату | 26.11.2023 р. | |
| 7. | Підготовка доповіді до захисту. | 15.12.2023 р. | |

Здобувач(ка) вищої освіти _____ Артем Кворижко
*(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Андрій СОБЧУК
*(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**
**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ**

**ПОДАННЯ**
**ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ**
**ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ**
**на здобуття освітнього ступеня магістра**

Направляється здобувач Коврижко А.О. до захисту кваліфікаційної роботи
(прізвище та ініціали)

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

на тему: «Підвищення можливостей виявлення загроз корпоративній інформаційній системі на прикладі QRadar Use Case Manager»

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Віталій САВЧЕНКО
(*підпис*) (*Ім'я, ПРІЗВИЩЕ*)

**Висновок керівника кваліфікаційної роботи**

Здобувач ***КОВРИЖКО Артем*** обрав тему роботи, метою якої було дослідити та проаналізувати сучасні загрози для корпоративних інформаційних систем, рішення для виявлення та протидії загрозам QRadar Use Case Manager та розробив власну систему виявлення та протидії сучасним загрозам сьогодення . Перелік використаних джерел свідчить про гарне знання англійської мови вміння знаходити потрібну інформацію, користуватися репозиторіями та тематичними форумами та навіть побудувати власну систему виявлення та протидії загрозам. Під час виконання кваліфікаційної роботи ***КОВРИЖКО Артем*** показав гарну теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***КОВРИЖКО Артема*** на оцінку **«відмінно»** та присвоїти йому кваліфікацію магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Андрій СОБЧУК
*(підпис)* *(Ім'я, ПРІЗВИЩЕ)*
"____" _____ 2023 року

**Висновок кафедри про кваліфікаційну роботу**

Кваліфікаційна робота розглянута. Здобувач(ка) ***КОВРИЖКО Артема.*** допускається до захисту даної роботи в Державній екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Галина ГАЙДУР
*(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

**ВІДГУК РЕЦЕНЗЕНТА**
на кваліфікаційну роботу

здобувача Коврижко Артема
на тему: «Підвищення можливостей виявлення загроз корпоративній інформаційній системі на прикладі QRadar Use Case Manager».

**Актуальність:**

Метою кожної організації є забезпечення безпеки власної інформаційної системи, основою такої безпеки є своєчасне виявлення загроз. Отримання доступу до інформаційної системи організації, може призвести до руйнації активів, репутації організації. Тому за останній час не аби якої популярності серед компаній набули комплексні рішення безпеки з Use Case. Одним з таких рішень є QRadar Use Case Manager, яке є комплексом технологій моніторингу та аналітики подій та реагування на них за вже готовими сценаріями, це дозволяє пасивно без втручання інженера захистити інформаційну систему від загроз. Тому тема кваліфікаційної роботи є актуальною та своєчасною.

**Позитивні сторони:**

1. На основі проведеного аналізу, в роботі встановлено зміст проблеми не своєчасного або взагалі не виявлення загроз корпоративній інформаційній системі.
2. Досліджено методи та засоби виявлення та протидії загрозам корпоративній інформаційній системі.
3. Проаналізовано варіант корпоративної інформаційної системи з розгорнутим QRadar Use Case Manager.
4. Розроблено варіант власної SIEM системи та дана методика розроблення таких систем.
5. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою магістерської роботи.

**Недоліки:**

1. У кваліфікаційній роботі доцільно було б більш детально описати процес створення власної SIEM та зібрати це в досконале opensource рішення.
2. Недостатньо порівняння QRadar Use Case Manager з іншими системами на прикладі розгортання на однакових полігонах та тестування їх можливостей .

**Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи**

**Висновок:** Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку «**відмінно»**, а здобувач **Коврижко Артем** - присвоєння кваліфікації магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Рецензент:
*д.т.н., професор* _____ *підпис* _____ *Ім'я, ПРІЗВИЩЕ*

# РЕФЕРАТ

Текстова частина кваліфікаційної роботи и на здобуття освітнього ступеня магістра: 76 сторінок, 18 рисунків, 2 таблиці, 14 джерел.

*Об'єкт дослідження* – процес виявлення загроз корпоративній інформаційній системі.

*Предмет дослідження* – технологія виявлення загроз на базі рішення QRadar Use Case Manager.

*Мета роботи* – розробити варіанти систем виявлення та протидії загроз корпоративній інформаційній системі на прикладі QRadar Use Case Manager.

*Методи дослідження* – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання корпоративної інформаційної системи та виявлення загроз для неї.

В роботі проведено аналіз проблеми виявлення загроз на основі MITRE ATT&CK. Проаналізовано існуючі технології та комплексні рішення виявлення загроз.

Досліджено методи та засоби виявлення та протидії загрозам.

Запропоновано варіант технології виявлення загроз на базі рішення QRadar Use Case Manager. Визначено призначення, основні функції та склад компонентів даної технології.

На основі проведених досліджень, в роботі розроблено варіант системи виявлення загроз на базі рішення QRadar Use Case Manager та розроблено свій варіант аналогічної системи.

Галузь використання – кібербезпека корпоративної мережі.

КОРПОРАТИВНА ІНФОРМАЦІЙНА СИСТЕМА, КІБЕРБЕЗПЕКА, ВИЯВЛЕННЯ ЗАГРОЗ, МЕТОДИ ТА ЗАСОБИ, MITRE ATT&CK, АРХІТЕКТУРА SIEM, МОДУЛІ, ФУНКЦІЇ

## ABSTRACT

Text part of the master's qualification work:76 pages, 18 figures, 2 tables, 14 sources.

*Object of research* - the process of identifying threats to the corporate information system.

*Subject of research* - threat detection technology based on the QRadar Use Case Manager solution..

*The purpose of the work* - develop variants of systems for detecting and countering threats to the corporate information system using the QRadar Use Case Manager as an example.

*Research methods* – study of the literature on this topic, analysis of operating documentation, international standards and their comparison, modeling of the corporate information system and identification of threats to it.

The paper analyzes the problem of threat detection based on MITER ATT&CK. Existing technologies and complex threat detection solutions are analyzed.The methods and means of managing network access of organizations have been studied.

Methods and means of detecting and countering threats have been studied.

A variant of threat detection technology based on the QRadar Use Case Manager solution is proposed. The purpose, main functions and composition of the components of this technology are determined.

On the basis of the conducted research, the paper developed a version of the threat detection system based on the QRadar Use Case Manager solution and developed its own version of a similar system.The field of use is cyber security of the corporate network.

CORPORATE INFORMATION NETWORK, CYBER SECURITY, , METHODS AND TOOLS,

DETECTION OF THREATS, MITRE ATT&CK, ARCHITECTURE SIEM, MODULES, FUNCTIONS

**ЗМІСТ**

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ПЗ – програмне забезпечення

ІТС – інформаційна телекомунікаційна система

ІБ – інформаційна безпека

ШПЗ – шкідливе програмне забезпечення

CISO – Chief Information Security Office

# ВСТУП

*Актуальність дослідження*. Сьогодні більшість підприємств, корпорацій та бізнесу починають використовувати інформаційні технології в усіх сферах людської діяльності, в усіх підприємствах є власні інформаційні системи, всі вони побудовані з використанням різних технологій з різними цілями, але всі вони мають спільну найбільшу проблему це вразливість до загроз.

Загрози виникають з різних причин, вони можуть бути пов’язані з тим чи іншим об’єктом інформаційної безпеки, виникають вони у процесі взаємодії між тим чи іншим об’єктом, або складовими цих об’єктів.

Загроза інформаційної безпеки — сукупність умов і факторів, що створюють небезпеку порушення інформаційної безпеки. Під загрозою (в загальному) розуміється потенційно можлива подія, дія (вплив), процес або явище, які можуть призвести до заподіяння шкоди чиїм-небудь інтересам.

Загрози умовно треба поділити на випадкові і навмиснеі, і їх треба чітко розділяти для забезпечення загальної безпеки в корпоративних інформаційних системах. Виявлення загроз є одним з найважливіших пріоритетів для забезпечення безпеки в в корпоративних інформаційних системах.

Сьогоднішні потреби інформатизації підприємств та корпорацій вимагають від комп’ютерних систем надвисокої стійкості до зовнішніх і внутрішніх загроз.

Підвищення виявлення загроз в корпоративних інформаційних системах є дуже поширеним запитом серед підприємств та компаній які мають власні інформаційні системи. Тому тема кваліфікаційної роботи є актуальною.

*Об’єкт дослідження* – процес виявлення загроз корпоративній інформаційній системі.

*Предмет дослідження* – технологія виявлення загроз на базі рішення QRadar Use Case Manager.

*Мета роботи* – розробити варіанти систем виявлення та протидії загроз корпоративній інформаційній системі на прикладі QRadar Use Case Manager.

*Наукові завдання:*

- провести аналіз питання щодо необхідності виявлення загроз корпоративній інформаційній системі;
- проаналізувати основні загрози корпоративній інформаційні системі;
- проаналізувати методи та засоби виявлення та протидії загрозам;
- розробити варіант системи виявлення та захисту від загроз в корпоративній інформаційній системі на базі рішення QRadar Use Case Manager та рекомендації щодо застосування даної технології.

*Методи дослідження* – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання корпоративної інформаційної системи та виявлення загроз для неї.

*Практичне значення одержаних результатів* полягає в розробці системи виявлення загроз на базі рішення QRadar Use Case Manager, рекомендації щодо застосування технології в залежності від особливостей організації, що дозволить забезпечувати необхідний рівень виявлення загроз інформаційній системі.

*Апробація результатів.* Результати даного дослідження доповідались на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки».

# 1 АНАЛІЗ ПРОБЛЕМИ ВИЯВЛЕННЯ ЗАГРОЗ КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИТСЕМІ

## 1.2. Аналіз проблеми загроз корпоративній інформаційній системі

Загроза інформаційної безпеки — сукупність умов і факторів, що створюють небезпеку порушення інформаційної безпеки. Під загрозою (в загальному) розуміється потенційно можлива подія, дія (вплив), процес або явище, які можуть призвести до заподіяння шкоди чиїм-небудь інтересам. Під загрозою інтересів суб'єктів інформаційних відносин розуміють потенційно можливу подію, процес або явище, яке з допомогою впливу на інформацію або інші компоненти інформаційної системи, може прямо або опосередковано призвести до заподіяння шкоди даним того чи іншого суб'єкта[1]

Загрози інформаційної безпеки можна класифікувати за певними ознаками:

- Загрози конфіденційності - загроза порушення конфіденційності полягає в тому, що інформація стає відомою тому, хто не володіє повноваженнями доступу до неї. Вона стається, коли отримано доступ до деякої інформації обмеженого доступу, що зберігається в комп'ютерній системі або передається від однієї системи до іншої.[1]
- Загрози порушення цілісності - це загрози, пов'язані з імовірністю модифікації тієї чи іншої інформації, що зберігається в інформаційній системі. Порушення цілісності може бути викликано різними чинниками — від умисних дій персоналу до виходу з ладу обладнання.[1]
- Загрози доступності - порушення доступності являє собою створення таких умов, при яких доступ до послуги або інформації або заблокований, або можливий за час, який не забезпечить виконання тих чи інших бізнес-цілей. [1]

Також поділити загрози можливо за розташуванням джерела на внутрішні та зовнішні. Внутрішні загрози виникають, коли працівники організації або інші люди які мають дозвіл на доступ до інформаційної системи або конфіденційної інформації, навмисно чи ненавмисно зловживають цим доступом, для того щоб негативно вплинути на роботу інформаційної системи організації.

Недбалі працівники, які не дотримуються бізнес-правил і політики безпеки своєї організації, створюють внутрішні загрози. Наприклад, вони можуть ненавмисно надати доступ до конфіденційних данних або навіть інформаційної системи, надсилати електронною поштою дані клієнтів стороннім особам, натискати фішингові посилання в електронних листах або ділитися своєю реєстраційною інформацією з іншими. Підрядники, ділові партнери та сторонні постачальники є джерелом інших внутрішніх загроз.

Деякі інсайдери навмисно обходять заходи безпеки через зручність або необдумані спроби підвищити продуктивність. Зловмисники навмисно ухиляються від протоколів кібербезпеки, щоб видалити дані, викрасти дані для подальшого продажу чи використання, порушити роботу чи іншим чином завдати шкоди бізнесу. [2]

За своїм походженням загрози можна поділити на випадкові та навмисні. Особливо уважно треба ставитись до загроз навмисних та вчасно їх виявляти. За результатами, які визначили фахівці з інформаційної безпеки досліджень, понад 65 % шкоди, що наноситься інформаційним ресурсам, є наслідком ненавмисних помилок. Це є підставою для акцентування уваги на ефективнішому впровадженні комп'ютерних систем для забезпечення безпеки. [1]

Залежно від різних способів класифікації, всі можливі загрози інформаційній безпеці можна розділити на основні підгрупи.

- Небажаний контент
- Несанкціонований доступ
- Витоку інформації

- Втрата даних
- Шахрайство
- Кібервійни
- Кібертероризм

Небажаний контент — це не лише шкідливий код, потенційно небезпечні програми та спам (тобто те, що безпосередньо створено для знищення чи крадіжки інформації), а й сайти, заборонені законодавством, а також небажані ресурси з інформацією, яка не відповідає віку споживача.

Несанкціонований доступ — перегляд інформації працівником, який не має дозволу користуватися нею шляхом перевищення посадових повноважень. Несанкціонований доступ призводить до витоку інформації. Залежно від того, які дані та де вони зберігаються, витоки можуть організовуватися різними способами, а саме через атаки на сайти, зламування програм, перехоплення даних по мережі, використання несанкціонованих програм.

Витоку інформації можна розділяти на навмисні та випадкові. Випадкові витоки трапляються через помилки обладнання, програмного забезпечення та персоналу. Умисні, у свою чергу, організовуються навмисно з метою отримати доступ до даних, завдати шкоди. Втрату даних вважатимуться однією з основних загроз інформаційної безпеки. Порушення цілісності інформації може бути викликане несправністю обладнання чи навмисними діями людей, чи то співробітники, чи зловмисники. Не менш небезпечною загрозою є шахрайство з використанням інформаційних технологій (фрод). До шахрайства можна віднести не лише маніпуляції з кредитними картками («кардинг » ) та злом онлайн-банку, а й внутрішній фрод. Цілями цих економічних злочинів є обхід законодавства, політики безпеки чи нормативних актів, присвоєння майна. Щороку в усьому світі зростає терористична загроза, поступово переміщуючись у віртуальний простір. Сьогодні нікого не дивує можливість атак на автоматизовані системи управління технологічними процесами різних підприємств. Але подібні атаки не проводяться без попередньої розвідки, для чого застосовується

кібершпигунство, що допомагає зібрати необхідні дані. Існує також таке поняття, як «інформаційна війна » ; вона відрізняється від звичайної війни тим, що як зброя виступає ретельно підготовлена інформація. Саме таку війну веде зараз РФ проти України.

Порушення режиму інформаційної безпеки може бути спричинене як спланованими операціями зловмисників, так і недосвідченістю співробітників. Користувач повинен мати хоч якесь поняття про ІБ, шкідливе програмне забезпечення, щоб своїми діями не завдати шкоди компанії та самому собі. Такі інциденти, як втрата або витік інформації, можуть бути обумовлені цілеспрямованими діями співробітників компанії, які зацікавлені в отриманні прибутку в обмін на цінні дані організації, в якій працюють або працювали.

Основними джерелами загроз є окремі зловмисники («хакери»), кіберзлочинні групи та державні спецслужби (кіберпідрозділи), які застосовують весь арсенал доступних кіберзасобів, перерахованих та описаних вище. Щоб пробитися через захист та отримати доступ до потрібної інформації, вони використовують слабкі місця та помилки в роботі програмного забезпечення та веб-додатків, вилучені в конфігураціях мережних екранів та налаштуваннях прав доступу, вдаються до прослуховування каналів зв'язку та використання клавіатурних шпигунів.

Те, чим буде здійснюватися атака, залежить від типу інформації, її розташування, способів доступу до неї та рівня захисту. Якщо атака буде розрахована на недосвідченість жертви, можливо, наприклад, використання спам-розсилок.

Оцінювати загрози інформаційної безпеки необхідно комплексно, у своїй методи оцінки відрізнятимуться у кожному даному випадку. Так, щоб унеможливити втрату даних через несправність обладнання, потрібно використовувати якісні комплектуючі, проводити регулярне технічне обслуговування, встановлювати стабілізатори напруги. Далі слід встановлювати та регулярно оновлювати програмне забезпечення (ПЗ). Окрему увагу потрібно приділити захисному програмному забезпеченню, бази якого повинні оновлюватися щодня.

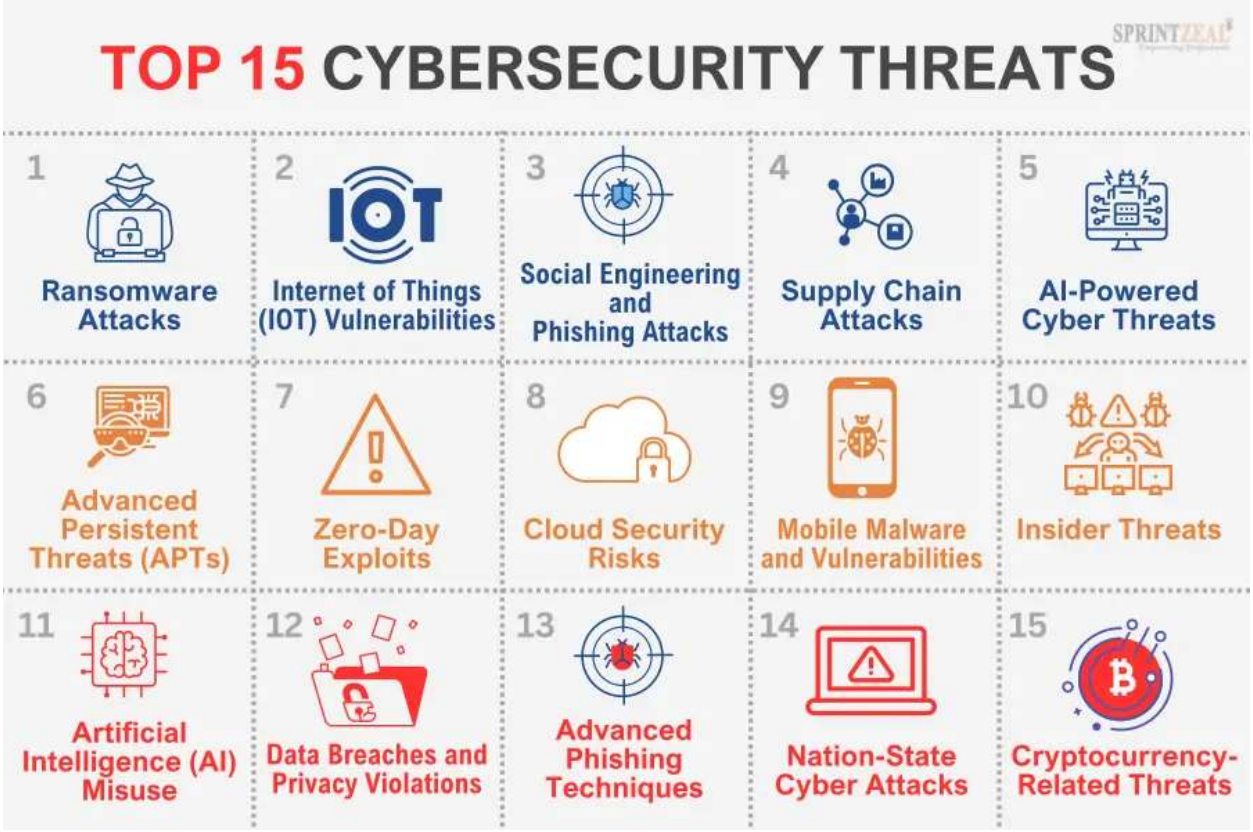



Рис 1.1. Топ 15 загроз для корпоративних інформаційних систем [5]

1. Атаки програм-вимагачів

Атаки програм-вимагачів залишаються поширеною загрозою в 2023 році. Кіберзлочинці продовжують удосконалювати свої методи, використовуючи розширене шифрування та цільові стратегії. Ці атаки можуть паралізувати організації, що призведе до значних фінансових втрат і шкоди репутації.

- Використовуйте вдосконалене шифрування та цільові стратегії
- Паралізує організації та призводить до значних фінансових втрат і репутаційної шкоди
- Захист від програм-вимагачів за допомогою надійних стратегій резервного копіювання, підвищення обізнаності співробітників і регулярних виправлень безпеки

2. Уразливості Інтернету речей (IoT).

Із поширенням пристроїв Інтернету речей розширюється зона атак для кіберзлочинців. У 2023 році вразливості Інтернету речей становлять значні ризики, оскільки багато пристроїв не мають належних заходів безпеки. Хакери можуть скористатися цими недоліками, щоб отримати неавторизований доступ або запустити розподілені атаки типу «відмова в обслуговуванні» (DDoS).

- Розширення поверхні атаки за рахунок поширення пристроїв IoT
- Відсутність належних заходів безпеки в багатьох пристроях IoT
- Пом'якшуйте вразливості IoT за допомогою надійних паролів, регулярних оновлень мікропрограми та сегрегації мережі

3. Соціальна інженерія та фішингові атаки

Соціальна інженерія та фішингові атаки залишаються дуже успішними у 2023 році. Кіберзлочинці використовують складні методи та персоналізовану інформацію, щоб обманювати людей. Велика кількість особистих даних, доступних у соціальних мережах та онлайн-платформах, робить ці атаки більш переконливими.

- Використовуйте складні методи та персоналізовану інформацію для обману окремих осіб
- Використовуйте велику кількість особистих даних, доступних у соціальних мережах та онлайн-платформах
- Протидіяйте атакам соціальної інженерії та фішингу за допомогою навчання з питань кібербезпеки, двофакторної автентифікації та обережного обміну інформацією

4. Supply Chain Attacks

Останніми роками атаки на ланцюги поставок набули популярності, і 2023 рік не став винятком. Проникаючи до надійних продавців або постачальників, хакери компрометують увесь ланцюжок поставок, потенційно впливаючи на численні організації.

- Скомпрометуйте весь ланцюжок постачання шляхом проникнення до надійних продавців або постачальників

- Вставте шкідливий код або бекдори в оновлення програмного забезпечення, які несвідомо розповсюджуються серед користувачів
- Запобігайте атакам на ланцюг поставок шляхом ретельної перевірки постачальників, регулярних оцінок безпеки та надійних протоколів реагування на інциденти

5. Кіберзагрози на основі ШІ

У 2023 році кіберзлочинці використовують штучний інтелект (ШІ) для організації складних атак. Загрози, керовані ШІ, автоматизують атаки, уникають виявлення та обходять традиційні заходи безпеки.

- Використовуйте штучний інтелект (AI) для організації складних атак
- Автоматизуйте атаки, уникайте виявлення та обходьте традиційні заходи безпеки
- Використовуйте рішення безпеки на основі штучного інтелекту та інвестуйте в захисні механізми на основі штучного інтелекту для протидії зловмисному штучному інтелекту

6. APT

APT — це складні довготривалі кібератаки, спрямовані на певні організації, наприклад уряди чи великі організації. У 2023 році APT продовжують становити серйозну загрозу, використовуючи приховані методи для отримання несанкціонованого доступу та підтримки стійкості в мережах.

- Складні довготривалі кібератаки, спрямовані на певні об’єкти
- Використовуйте приховані методи для отримання несанкціонованого доступу та підтримки стабільності в мережах
- Пом'якшуйте APT за допомогою сильного контролю доступу, регулярних оцінок безпеки та передових технологій виявлення загроз і реагування

7. Експлойти Zero-Day

Експлойти нульового дня націлені на раніше невідомі вразливості програмного забезпечення без доступних виправлень або засобів захисту. У 2023 році експлойти

нульового дня дуже затребувані в кібернетичному просторі злочинців і хакерів, які фінансуються державою.

- Націлюйтеся на раніше невідомі вразливості програмного забезпечення без доступних виправлень або засобів захисту
- Затребуваний кіберзлочинцями та хакерами, які фінансуються державою
- Захищайтеся від експлойтів нульового дня, оновлюючи програмні виправлення, використовуючи системи виявлення вторгнень і відстежуючи бази даних уразливостей

8. Cloud Security Risks

Широке впровадження хмарних сервісів створює нові ризики для безпеки. У 2023 році неправильна конфігурація, витік даних і неавторизований доступ до хмарних середовищ викликають значне занепокоєння.

- Поява нових ризиків безпеки з широким впровадженням хмарних сервісів
- Неправильні конфігурації, витоки даних і неавторизований доступ до хмарних середовищ викликають серйозне занепокоєння
- Надавайте пріоритет безпечним хмарним конфігураціям, надійній автентифікації та шифруванню та постійному моніторингу хмарних середовищ

9. Мобільні шкідливі програми та вразливості

Мобільні пристрої все частіше стають мішенями кіберзлочинців через їх широке використання та доступ до конфіденційної інформації. У 2023 році зловмисне програмне забезпечення та вразливості для мобільних пристроїв створюють значні ризики, зокрема витік даних і крадіжку особистих даних.

- Посилення націлювання на мобільні пристрої з боку кіберзлочинців через широке використання та доступ до конфіденційної інформації
- Ризики включають витік даних і крадіжку особистих даних
- Захищайте мобільні пристрої за допомогою надійних програм безпеки, регулярних оновлень операційної системи та обережного завантаження програм

10. Внутрішні загрози

Інсайдерські загрози стосуються зловмисних або недбалих дій окремих осіб в організації. У 2023 році внутрішні загрози залишаються серйозною проблемою, оскільки співробітники з привілейованим доступом можуть навмисно чи ненавмисно скомпрометувати дані та системи.

- Зловмисні або недбалі дії окремих осіб в організації
- Співробітники з привілейованим доступом можуть скомпрометувати дані та системи
- Запобігайте та виявляйте внутрішні загрози за допомогою суворого контролю доступу, моніторингу діяльності співробітників та регулярного навчання з кібербезпеки

11. Зловживання штучним інтелектом (AI).

Хоча штучний інтелект має багато корисних застосувань, він також може бути використаний у зловмисних цілях. У 2023 році зловживання ШІ створює зростаючу загрозу кібербезпеці. Кіберзлочинці можуть використовувати алгоритми ШІ для автоматизації атак, покращення тактики соціальної інженерії або обходу систем безпеки.

- Зловживання штучним інтелектом у зловмисних цілях є зростаючою загрозою кібербезпеці
- Алгоритми ШІ можуть автоматизувати атаки, покращити тактику соціальної інженерії або обійти системи безпеки
- Пом'якшуйте зловживання штучним інтелектом, запроваджуючи рамки етики штучного інтелекту, проводячи аудит моделі штучного інтелекту та відстежуючи підозрілі дії в системах штучного інтелекту.

12. Витоки даних і конфіденційності

У 2023 році витік даних і порушення конфіденційності залишаться основною проблемою кібербезпеки. Щоб отримати конфіденційні дані, кіберзлочинці атакують бізнес, що може завдати величезної фінансової та репутаційної шкоди. Підприємства

повинні надавати пріоритет захисту даних через законодавчі обмеження щодо конфіденційності даних.

- Порушення даних та конфіденційності становлять значні ризики у 2023 році
- Кіберзлочинці націлені на організації, щоб викрасти конфіденційні дані
- Захист від витоку даних і порушень конфіденційності за допомогою надійного шифрування даних, контролю доступу та регулярних перевірок безпеки

13. Розширені методи фішингу

У 2023 році фішингові атаки розвинулися з використанням більш складних методів. Кіберзлочинці використовують передові тактики соціальної інженерії, добре продумані електронні листи та реалістичні підроблені веб-сайти, щоб обманом змусити людей розкрити конфіденційну інформацію. Ці атаки спрямовані як на окремих осіб, так і на організації, тому вкрай важливо залишатися пильним.

- Фішингові атаки використовують передову тактику соціальної інженерії у 2023 році
- Добре продумані електронні листи та реалістичні підроблені веб-сайти обманом змушують людей розкрити конфіденційну інформацію
- Захист від просунутих методів фішингу за допомогою фільтрації електронної пошти, навчання користувачів і антифішингового програмного забезпечення

14. Кібератаки на національну державу

Уряди, організації та ключова інфраструктура піддаються серйозній загрозі через кібератаки національних держав у 2023 році. Ці напади планують добре забезпечені ресурсами та досвідчено підготовлені кібергрупи з наміром порушити або проникнути в мережі з комерційною, військовою чи політичною вигодою.

- Кібератаки національних держав становлять значну загрозу у 2023 році
- Керується добре фінансованими та висококваліфікованими кіберпідрозділами

- Пом'якшуйте кібератаки національних держав за допомогою надійної безпеки мережі, планування реагування на інциденти та обміну інформацією про загрози

15. Загрози, пов’язані з крипто валютою

Зростання криптовалют у 2023 році спричинило нові загрози кібербезпеці. Кіберзлочинці націлюються на біржі криптовалют, гаманці та транзакції, щоб викрасти кошти або здійснити атаки зловмисників. Децентралізована та анонімна природа криптовалют ускладнює відстеження та повернення вкрадених активів.

- У 2023 році загрози, пов’язані з криптовалютою, є помітними
- Кіберзлочинці націлені на біржі, гаманці та транзакції з метою отримання фінансової вигоди
- Захист від загроз, пов’язаних із криптовалютою, за допомогою безпечного керування гаманцем, двофакторної автентифікації та обережної участі в початкових пропозиціях монет (ICO)

## 1.2. Аналіз проблеми виявлення загроз корпоративній інформаційній системі

В результаті великого технологічного прогресу наше середовище постійно змінюється. Зараз, як ніколи, люди та організації покладаються на технології, щоб зробити життя більш динамічним. І ця залежність від технологій і, як наслідок, розширення площі атаки – це те, на що кіберзлочинці роблять ставку, створюючи загрози, які мають на меті обдурити користувачів і організації.

Візьмемо, наприклад, те, як організації прагнуть зробити процеси більш оптимізованими та зручними. Ось чому все більше компаній використовують DevOps — щоб підвищити ефективність і масштабованість своїх продуктів і послуг. Але зловмисники постійно розробляють низку атак, як-от розгортання програм-вимагачів і використання методів впровадження зловмисного коду мільйонів людей.завантажте

ідентифікаційну інформацію (PII) або майнінгу криптовалюти які скорочують час виробництва та завдають фінансової шкоди підприємствам. Крім цих загроз, неправильна конфігурація залишається причиною руйнування багатьох організацій, які використовують хмарні програми та платформи, що дозволяє кіберзлочинцям отримувати незаконний доступ до кіберассетів для

Проблема виявлення загроз на сьогоднішній день є основною для забезпечення безпеки від загроз корпоративнй інформаційній системі. Щодня реєструється понад 450 000 нових шкідливих програм (malware) і потенційно небажаних програм (PUA). Їх перевіряють і класифікують відповідно до їхніх характеристик і зберігають. Потім програми візуалізації перетворюють результати на діаграми, які можна оновлювати та створювати поточну статистику зловмисного програмного забезпечення.

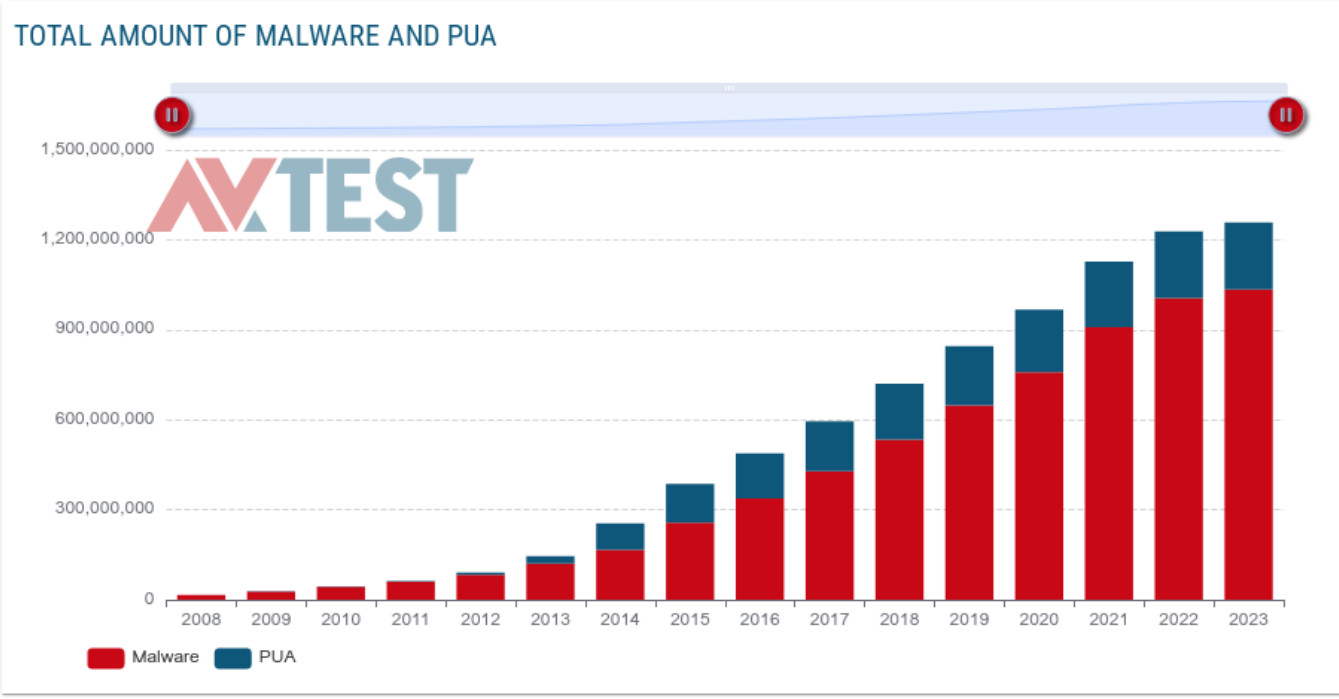



Рис 1.2. Загальна кількість зловмисних програм [11]

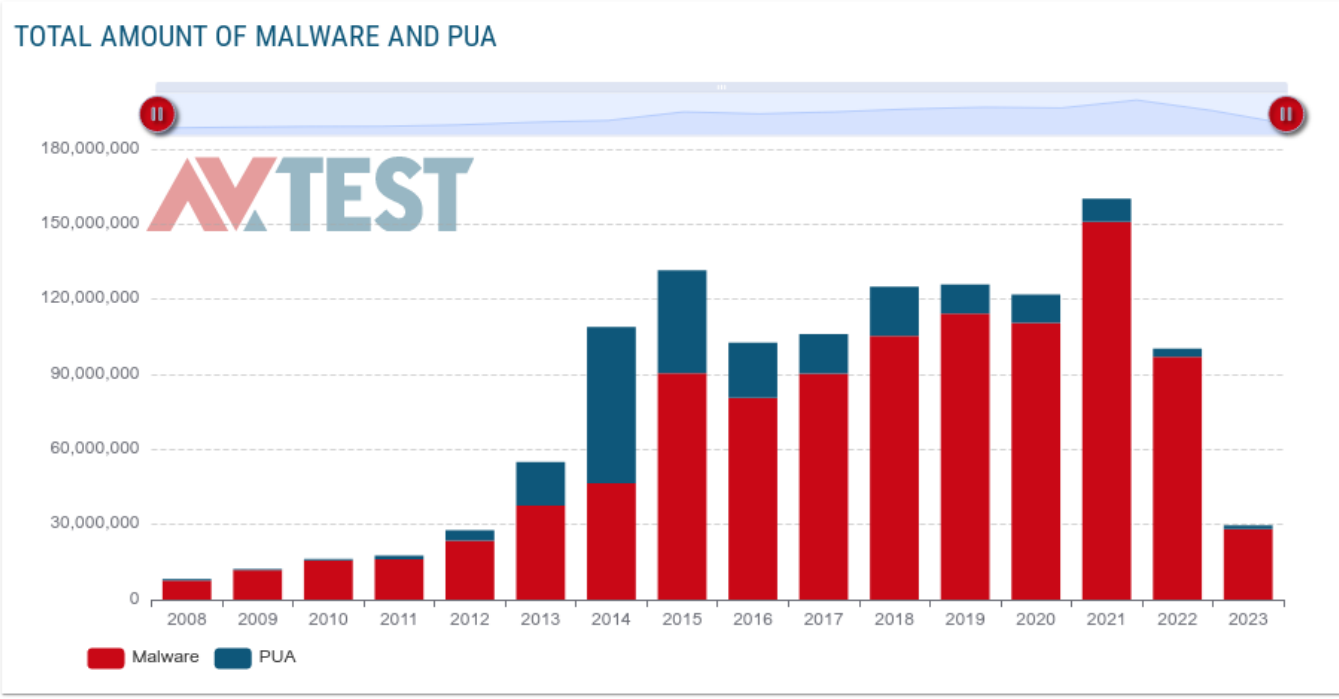



Рис 1.3. Нові зловмисні програми [11]

На діаграмах ми бачимо що перед компаніями кожен день постають нові загрози, зловмисники кожен день намагаються розробити нові підходи, методи та тактики щоб проникнути не поміченими в корпоративні інформаційні системи.

Більшість варіантів ШПЗ актуальні тільки короткий час після їх виготовлення, але часто зловмисники беруть вже готові рішення та модернізують їх намагаючись обійти системи виявлення загроз.

Інформаційні системи компаній продовжують перебувати під постійним потоком нових атак і варіантів зловмисного програмного забезпечення. Насправді, згідно з останніми дослідженнями, лише у 2021 році з'явилося понад 170 мільйонів нових варіантів зловмисного програмного забезпечення. Як наслідок, навантаження на CISO та їхні команди щодо виявлення та припинення цих нових загроз ніколи не було таким великим. Але при цьому вони стикаються з різними проблемами: нестачею навичок, кореляцією даних вручну, пошуком помилкових спрацьовувань, тривалими розслідуваннями тощо. У цій статті я хотів би вивчити деякі проблеми програми

виявлення загроз, з якими стикаються CISO, і надати кілька порад щодо покращення своїх операцій безпеки.

Ми розберемо ключові проблем, які можуть вплинути на виявлення загроз в корпоративній інформаційній системі, і як CISO повинні діяти перед своєю організацією, групою безпеки та постачальниками, які пропонують рішення для їх вирішення.

- У мережі надто багато індикаторів зламу (IoC) або подій безпеки, щоб належним чином визначити зловмисну активність. У результаті CISO шукають передові інструменти, які можуть співвідносити й ефективно аналізувати ці дані, щоб усунути помилкові спрацьовування. Останнє, чого хоче будь-який CISO, це щоб його/її команда витрачала час на подію, яка може бути просто невдалим входом, пов’язаним із тим, що користувач кілька разів неправильно ввів свій пароль.
- Співвідносити дані в часі важко. Це як складати шматочки пазла з коробки, наповненої кількома пазлами. Напад, який стався один раз, може бути досить важко ідентифікувати. Але як тільки суб’єкти загрози потрапляють у середовище, вони часто виконуватимуть невелику діяльність, розподілену на довший період (іноді через дні, тижні чи місяці). Це робить майже неможливим для людини-аналітика провести ці, здавалося б, різні події в часі та з’єднати їх, щоб завершити головоломку. Більшості інструментів також важко співвіднести ці, здавалося б, незалежні події як частину однієї атаки, оскільки вони здаються не пов’язаними з часом. CISO відповідають за те, щоб у команди було все необхідне (виходячи з обмежених бюджетів), щоб скласти пазл до того, як буде завдано збитків.
- Під час створення кампанії атаки вручну кореляція та дослідження різних джерел безпеки значно збільшує час і ресурси, необхідні CISO та його/її команді. Щоб отримати контекстну інформацію, необхідну для того, щоб дізнатися, що не так (і як реагувати), необхідно отримати дані з кількох систем одночасно. Але за цей час шкода вже може бути завдана. Ця проблема може легко розчарувати CISO, які інвестували стільки часу та грошей у створення програми безпеки.

- Проблемою залишається нестача навичок. Однак, оскільки більш досвідчені практики, які пройшли фундаментальну підготовку з мереж, серверів та інших аспектів IT, старіють із робочої сили, CISO змушені наймати більше аналітиків, орієнтованих на безпеку, але з меншим практичним досвідом.
- Постачальники надто багато обіцяють і не виконують. Коли йдеться про виявлення загроз, занадто багато постачальників неправдиво заявляють або перебільшують, що вони мають машинне навчання, штучний інтелект багатохмарну підтримку, та застосування показників ризику. CISO стикаються з постачальниками, які стверджують, що пропонують ідеальне рішення, а по факту таким воно не є, дуже часто використовують сумнівні маркетингові заяви про штучний інтелект і тому подібне. В найкращому випадку жоден постачальник не забезпечує те, що обіцяно.
- Компроміс між витратами та бюджетом і кращою безпекою може бути болісним вибором. CISO часто пропонують платформи (наприклад, SIEM), які стягують з організацій плату залежно від обсягу отриманих даних. У міру зростання організації стягнення плати за отримані дані є непередбачуваним і може швидко призвести до швидкого зростання витрат на ліцензування та зберігання. Як наслідок, CISO повинні шукати рішення, які зменшують цей тягар витрат, водночас дозволяючи організації отримувати та приймати якомога більше даних.
- Автоматизація може підвищити ефективність і прискорити виявлення загроз. Це може звільнити членів групи безпеки, щоб зосередити свою увагу на більш інтенсивних завданнях. Якщо це зробити ефективно, це забезпечує економію операційних витрат, що означає менше часу та ресурсів, витрачених на прості та ручні завдання невеликої вартості, а також скорочує час для виконання завдань високої вартості. Це також може надати кращий досвід для молодших аналітиків, особливо коли ваша аналітика та автоматизація прозорі, дозволяючи їм навчатися та вдосконалюватися.

Ще одна подія — дедалі більша кількість пристроїв IoT. Ці інтелектуальні пристрої підтримують бездротовий зв’язок удома, перетворюючи повсякденні справи

на безперебійну й автоматизовану щоденну роботу. Вони також відіграють важливу роль у зміні світу праці, коли дистанційна робота та програми «принеси свій власний пристрій» (BYOD) тепер стають нормою. Однак ці пристрої можна зламати — поставити під загрозу безпеку й конфіденційність користувачів, а також критичні та чутливі активи компаній. Кіберзлочинці можуть компрометувати пристрої IoT та створити зловмисну ботнет, яку потім можна використовувати для націлювання на сервери та надсилати величезну кількість спам-листів, які містять зловмисне програмне забезпечення. Якщо залишити без захисту, пристрої, які спрощують завдання, можуть бути тими самими речами, які піддають ризику користувачів і дані.

Через складність сучасних загроз організації мають труднощі з точним і своєчасним виявленням і розслідуванням загроз, навіть якщо існують рішення для виявлення та реагування на кінцеві точки (EDR), особливо якщо ці рішення не забезпечують такої швидкості, як широка видимість усієї підключеної інфраструктури підприємства. Окрім цього, організації можуть мати низку продуктів кібербезпеки, які створюють багато даних, які потребують значних ресурсів, часу та фінансів для ефективного підтримувати й аналізувати.

Навіть з кваліфікованим персоналом у розпорядженні організації величезний обсяг завдань, пов’язаних із розслідуванням проблем і просіюванням сірих сповіщень вимагає часу, можна витратити на зміцнення та покращення їх інфраструктури. І оскільки організації використовують нові додатки та програмне забезпечення для подальшого стимулювання інновацій та операцій, внутрішні спеціалісти з кібербезпеки залишаються все більш завалені. Не кажучи вже про те, як кіберзлочинці продовжують розвивати свої атаки, щоб уникнути виявлення або підтримувати стійкість систем, від стеганографії до безфайлової техніки.

Очевидно, що динамізм виявляється не лише в технологіях, які стимулюють продуктивність, але й у викликах і загрозах безпеці. Це лише означає, що кібербезпека також має бути динамічною.

## 1.3. Аналіз існуючих засобів та методів виявлення загроз корпоративній інформаційній системі

В сучасному світі високої інформатизації суспільства та бізнесу, компаній та корпорацій, постає слушне питання вибору правильних засобів та методів захисту від загроз, але першим чином загрози треба виявити це сонова успішного захисту, тому розберемо існуючі методи та засоби виявлення загроз.

З кожним новим витоком даних або кібератакою складність виявлення загроз і реагування на них зростає, а тиск на команди безпеки підприємства посилюється. Справа в тому, що виявлення загроз є складним і, згідно з нещодавнім опитуванням ESG Research, стає ще більш складним. Частково спонсороване Symantec опитування ESG серед керівників корпоративної кібербезпеки показало, що понад три чверті (76%) опитаних вважають, що виявлення загроз і реагування на інциденти сьогодні складніше, ніж це було лише два роки тому. Це вражаючий результат, особливо враховуючи величезну кількість уваги, ресурсів та інвестицій, витрачених протягом останніх кількох років на оборонні стратегії та продукти кібербезпеки, і потенційно є доказом того, що в майбутньому ситуація може тільки погіршитися.

Опитування ESG викликає запитання: чому процеси виявлення загроз і реагування на них такі складні? Я вважаю, що відповіді одночасно прості та складні. Проблема полягає лише в тому, що кібератаки продовжують зростати в масштабах і витонченості. Простіше кажучи, вони ніколи не закінчуються, і їх стає все важче виявити.

Тенденції кібербезпеки останнім часом - масові кібератаки, хакери з сходу атакують нашу критичну інфраструктуру, дефіцит фахівців через війну і еміграцію багатьох з них, законодавчі норми - диктують українському ринку ІБ-рішень та послуг нові вимоги: SOC-центри, послуги MSS-провайдерів, рішення класів SIEM та XDR, системи автоматизації реагування на інциденти та управління даними про кіберзагрози. Тому ми порівняємно продукти класів SIEM, SOAR, XDR, TIP, SGRC –

всі ці рішення активно використовуються SOC-центрами та командами реагування для ефективної обробки кіберінцидентів, автоматизації своєї діяльності, надсилання звітності щодо інциденті.Опишемо кожен з класів та дамо стислу характеристику.

Рішення SIEM (Security Information and Event Management, системи управління інформацією про безпеку та події ІБ) призначені для збору даних про події ІБ та зміни в інформаційній інфраструктурі для виявлення кіберинцидентів на основі кореляційної логіки з використанням методів обробки одержуваної з різнорідних джерел інформації (парсинг, нормалізація , Таксономія). Перші рішення класу SIEM з'явилися на міжнародному ринку ще наприкінці 90-х, але особливої популярності набули наприкінці 2010-х, коли у замовників з'явилося розуміння доцільності експлуатації загалом недешевих рішень, а на ринок вийшли великі гравці, підхопивши тренд, та необхідність виконання замовниками регуляторних норм щодо моніторингу подій ІБ.


Рис 1.4. Схема роботи SIEM

Рішення SOAR (Security Orchestration, Automation and Response, платформи для координації та управління СЗІ, автоматизації дій аналітиків та реагування на інциденти) призначені для комплексної автоматизації управління кіберінцидентами – від підготовки до реагування та первинного аналізу інциденту до загроз після атаки. SOAR-рішення використовують розроблені сценарії реагування на інциденти та управління інтегрованими СЗІ та інфраструктурними компонентами (мережевими пристроями, кінцевими точками). Завдяки тому, що в SOAR агрегується вся релевантна інциденту інформація та всі дії виконуються з єдиного інтерфейсу, значно прискорюється проведення аналізу та реагування, а аналітик ІБ або працівник SOC-

центру ефективно розподіляють свої ресурси. В даний час на рішення класу SOAR відзначається високий попит як з боку SOC-центрів, так і з боку MSS-провайдерів, для яких швидкість виявлення та реагування на інциденти є критично важливою, а дефіцит кібераналітиків став уже хронічним.

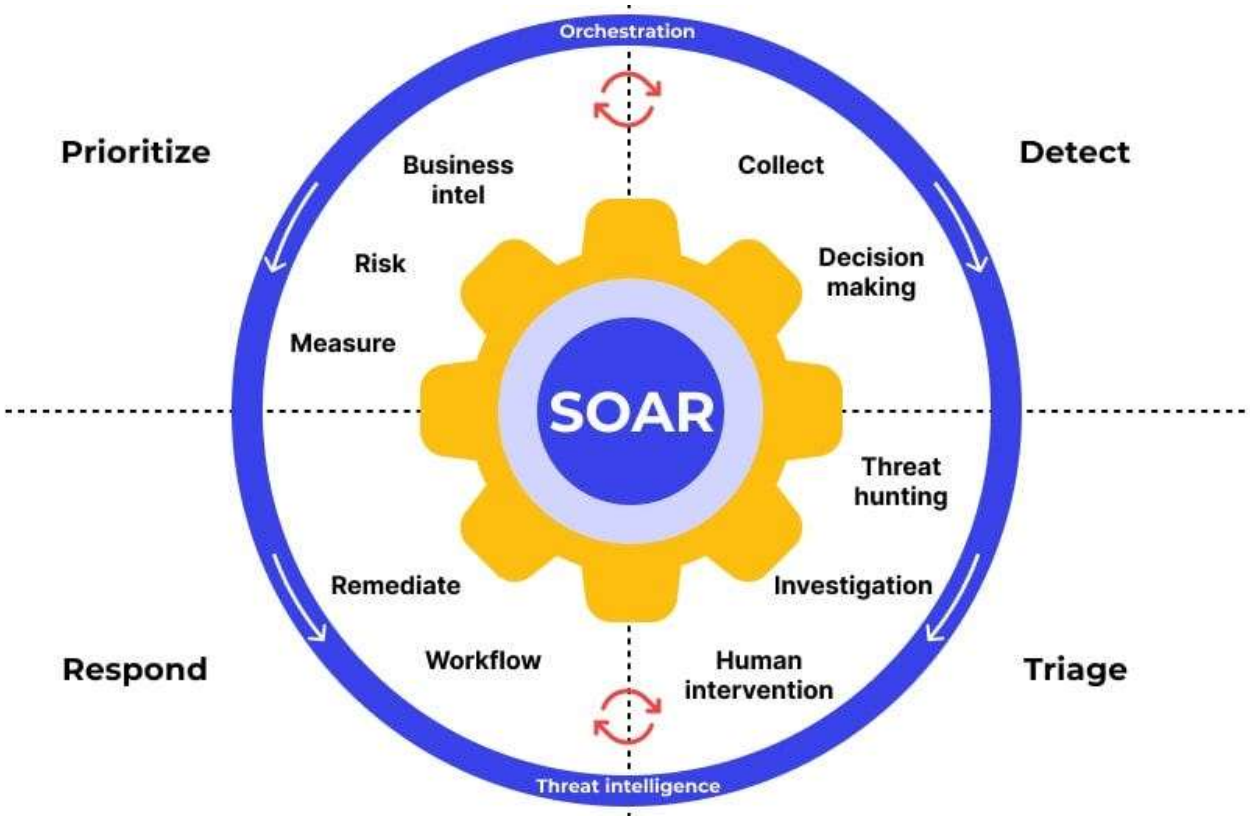



Рис 1.5. Схема роботи SOAR

Рішення XDR (Extended Detection and Response, системи розширеного виявлення та реагування на кібератаки) призначені для виявлення інцидентів та активного реагування (стримування, усунення загрози). В основі XDR-рішень лежать кілька продуктів від одного вендора, об'єднані єдиною логікою та методами керування інцидентами. Як правило, виявлення та реагування відбувається за рахунок моновендорної інтеграції EDR-продукту (розширений захист кінцевих точок), рішень щодо захисту email та корпоративної мережі (NTA/NDR/SWG), рішень щодо захисту облікових записів та хмарних інфраструктур, системи управління вразливістю," пісочниці", даних кіберрозвідки та SIEM-системи. XDR-рішення в чомусь конкурують із системами SOAR в частині автоматизації виявлення та реагування на

кіберзагрози, проте SOAR-рішення вендоронезалежні і передбачають інтеграцію в інфраструктуру, що вже склалася, без необхідності заміщення наявних СЗІ. Однак, компоненти XDR-рішення глибше інтегровані між собою (завдяки єдиному виробнику), і підійдуть тим, хто будує «з нуля» моновендорну ІБ.

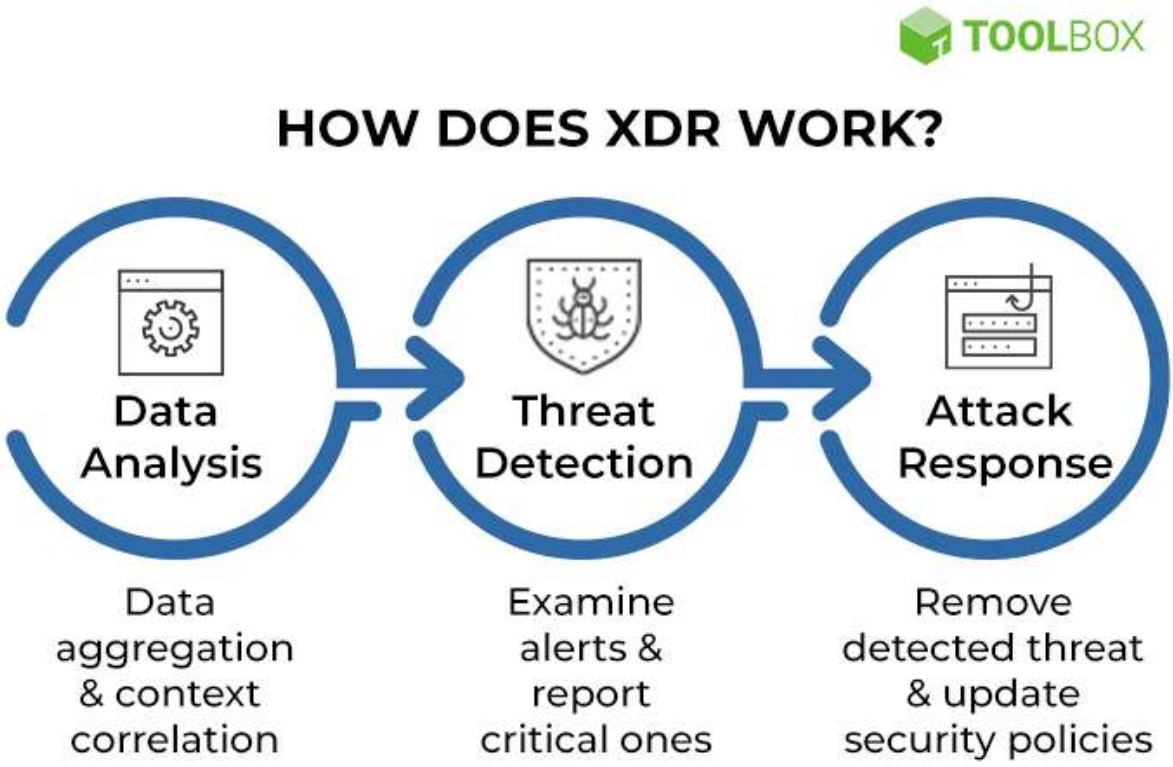



Рис 1.6. Схема роботи XDR

Рішення TIP (Threat Intelligence Platform, платформи управління інформацією про кіберзагрози) застосовуються для збору аналітичних даних про кіберзагрози, які надходять від джерел – фідів Threat Intelligence (антивірусні лабораторії, групи CERT, ІБ-компанії, незалежні дослідники). Аналітичними даними можуть бути індикатори компрометації (скорочено IoC, Indicator of Compromise: шкідливі IP-адреси та URL, хеші файлів ВПО тощо), індикатори атак (скорочено IoA, Indicator of Attack: використовувані атакуючими тактики, техніки та процедури TTPs - Tactics, Techniques and Procedures, тобто характерний "почерк" різних кіберзлочинних груп), а також інші структуровані та неструктуровані дані, що стосуються кібератак, такі як бюлетені

безпеки, опис вразливостей та експлойтів, зміст постів у месенджерах, соцмережах та на Даркнет-форумах тощо. У TIP отримана інформація класифікується, перевіряється, пріоритизується залежно від її релевантності для конкретного замовника та інфраструктури. Вендори TIP-рішень можуть використовувати як власні TI-фіди, так і сторонні (комерційні та безкоштовні) – різниця як отримані дані та необхідність їх додаткового аналізу. На відміну від інших розглянутих рішень, якість даних кіберрозвідки суттєво залежить від контексту, галузі та географічного розташування потенційних жертв атаки – наприклад, західні кіберзлочинці рідко атакують українські компанії, а східні виробники та TI-постачальники можуть навмисно приховувати індикатори кіберкампаній щодо іноземних спецслужб.

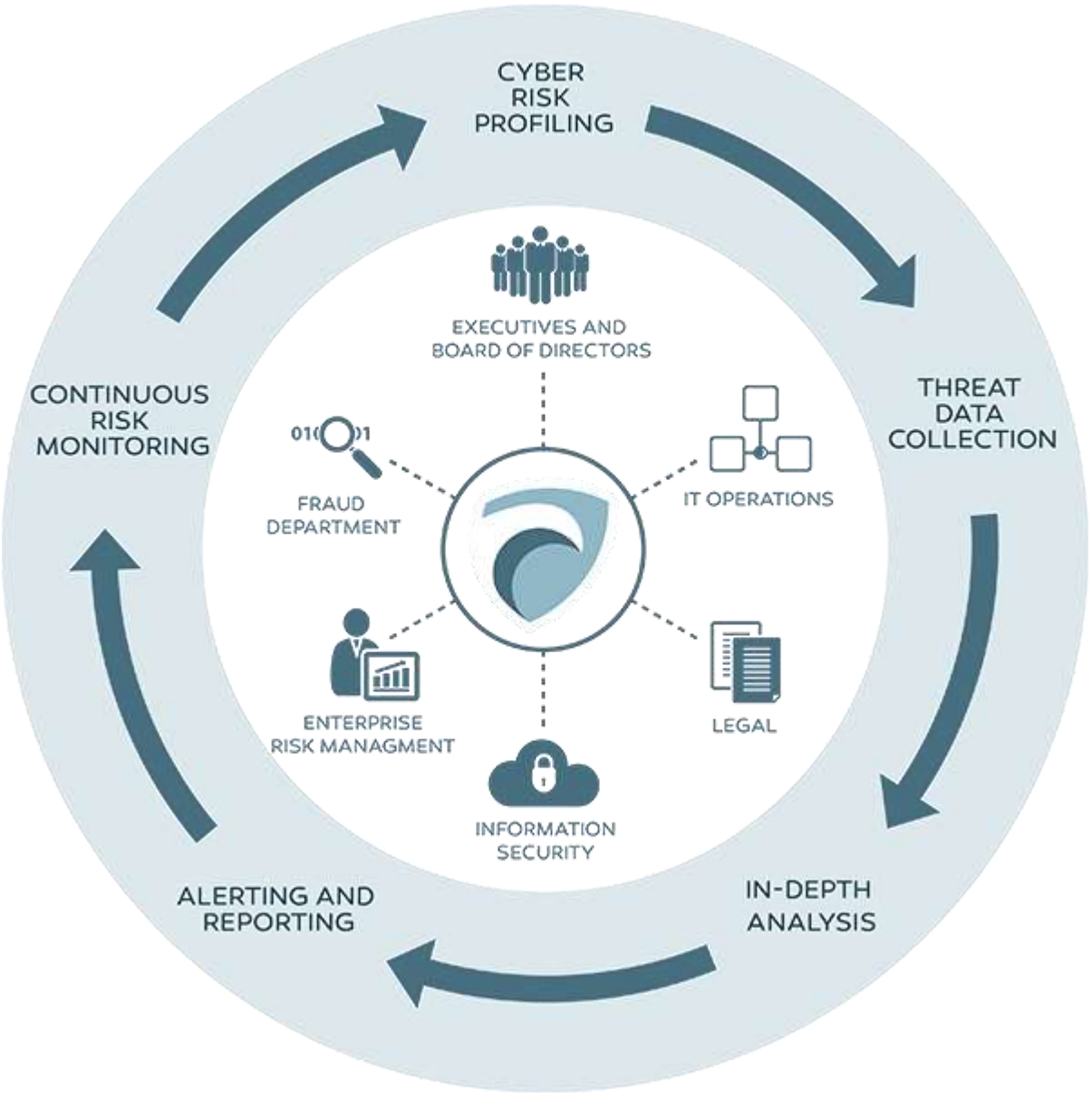



Рис 1.7. Схема роботи TIP

Рішення SGRC (Security Governance, Risk and Compliance, системи управління кібербезпекою, кіберрисками та відповідністю законодавству) застосовуються для автоматизації безлічі процесів, пов'язаних із системою управління ІБ у компаніях: наприклад, управління активами, уразливістю, конфігураціями, проведення аудитів (зовнішніх) самооцінка відповідності застосовним нормам ІБ-законодавства, управління кіберрисками. У контексті роботи SOC-центрів застосування SGRC-систем може бути доцільним через необхідність управління процесами самого SOC, а також ІБ-процесами організації, що захищається (якщо це входить у зону

відповідальності SOC). SGRC допоможе проаналізувати кіберриски самого SOC та ступінь відповідності процесів SOC внутрішнім регламентам, оцінити та візуалізувати виконання KPI, а також виконати законодавчі вимоги щодо відправки звітності по вимогам законодавства. Спеціалізація SGRC-рішень на виконанні норм законодавства дозволяє виробникам цих рішень своєчасно актуалізувати необхідні шаблони документів та звітів, базу застосовних нормативних актів та вимог, підтримувати інтеграцію для автоматизованих способів обміну інформацією з регуляторами.


Рис 1.8. Схема роботи GRC

Навчання співробітників компанії основним поняттям інформаційної безпеки та принципам роботи різних шкідливих програм допоможе уникнути випадкових витоків даних, виключити випадкове встановлення потенційно небезпечного програмного забезпечення на комп'ютер. Також як запобіжний засіб від втрати

інформації слід робити резервні копії. Для того, щоб стежити за діяльністю співробітників на робочих місцях та мати можливість виявити зловмисника, слід використовувати DLP-системи.

Організувати інформаційну безпеку допоможуть спеціалізовані програми, розроблені на основі сучасних технологій:

- захист від небажаного контенту (антивірус, антиспам, веб-фільтри, антишпигуни);
- мережеві екрани та системи виявлення вторгнень (IPS);
- керування обліковими даними (IDM);
- контроль привілейованих користувачів (PUM);
- захист від DDoS; захист веб-додатків (WAF);
- аналіз вихідного коду; антифрод;
- захист від таргетованих атак; управління подіями безпеки (SIEM); системи виявлення аномальної поведінки користувачів (UEBA);
- захист АСУ ТП; захист від витоків даних (DLP);
- шифрування; захист мобільних пристроїв; резервне копіювання; системи відмовостійкості.

# 2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ ЗАГРОЗ КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

## 2.1. Аналіз пішення QRadar Use Case Manager та його особливості

Use Case в загальному розумінні це не окремий компонент, а чистина повноцінного рішення у вигляді SIEM. Для повного розуміння сутності QRadar Use Case Manager потрібно визначитись зі значенням SIEM до якої він відноситься.

SIEM (Security Information & Event Management) — програмно-апаратний комплекс для збору інформації про події (логи), їх кореляцію та аналіз.

Рішення SIEM призначені для збору даних про події ІБ та зміни в інформаційній інфраструктурі для виявлення кіберинцидентів на основі кореляційної логіки з використанням методів обробки одержуваної з різнорідних джерел інформації (парсинг, нормалізація , Таксономія). Перші рішення класу SIEM з'явилися на міжнародному ринку ще наприкінці 90-х, але особливої популярності в Росії набули наприкінці 2010-х, коли у замовників з'явилося розуміння доцільності експлуатації загалом недешевих рішень, а на ринок вийшли вітчизняні гравці, підхопивши тренд на імпортозаміщення. та необхідність виконання замовниками вітчизняних регуляторних норм щодо моніторингу подій ІБ. До цього огляду ми включили ключових учасників вітчизняного SIEM-ринку: Kaspersky Unified Monitoring and Analysis Platform (KUMA) від Лабораторії Касперського та MaxPatrol SIEM від Positive Technologies. Крім них, були включені й інші гравці: RuSIEM та R-Vision SIEM – на жаль, R-Vision практично в останній момент відмовилася від участі в огляді за своїм SIEM-рішенням (а знайти референсні джерела нам не вдалося), але представила свої продукти в інших категоріях огляду. Більше того, до огляду включено західне рішення IBM QRadar для порівняння можливостей цього продукту

з більш ніж 20-річною історією з функціоналом російських SIEM, що з'явилися наприкінці 2010-х.[5]

У контексті безпеки варіант використання відноситься до конкретного сценарію або ситуації, яка описує, як система або рішення безпеки реагуватиме на певну подію або набір подій. Варіанти використання зазвичай використовуються при проектуванні, розробці та тестуванні систем безпеки, щоб переконатися, що вони відповідають конкретним вимогам безпеки та цілям.

Use Case (стосовно SIEM) — усталений термін, що означає певний набір правил/скриптів та/або механізмів візуалізації. Наприклад, для виявлення сканування портів, звірки IP-адреси за зовнішньою базою репутації і т.д. Use Cases можна написати самостійно, взяти готові із сайту виробника або замовити у підрядників.

QRadar Use Case Manager включає дослідник варіантів використання, який пропонує гнучкі звіти, пов’язані з вашими правилами. Додаток також надає попередньо визначені зіставлення MITER із системними правилами та допомагає вам зіставляти ваші власні правила з тактикою та технікою MITER ATT&CK.[2]

До складу QRadar Use Case Manager входить браузер варіантів використання з гнучкими звітами за правилами. Крім того, QRadar Use Case Manager пропонує стандартні відображення в системні правила і допомагає пов'язати ваші власні правила користування з тактиками і прийомами MITRE ATT&CK. MITRE ATT&CK є одним з найважливіших та найпотрібніших компонентів в QRadar Use Case Manager.[3]

MITRE ATT&CK - систематизований опис технік (прийомів) та тактик, які використовують зловмисники при атаках на організації. Ця методологія дозволяє забезпечити належний рівень захисту та своєчасно виявити атаки на інфраструктуру, а також дає розуміння того, на якому етапі шкідливої операції знаходяться хакери, яку мету вони мають і яким способом можна виявити їхню присутність. Якщо розглядати MITRE ATT&CK комплексно, то це не тільки матриці тактик і технік, але також інформація про джерела даних, що застосовуються для виявлення дій кіберзлочинців,

про способи зниження ризиків в інформаційній безпеці, про злочинні угруповання, шкідливі програми, що ними використовуються, і хакерські кампанії.

Матриці MITRE ATT&CK складаються з двох складових це тактика та техніка. Сутність тактики це визначити мету яку прагнуть досягти атакуючі шляхом певних технік та процедур. Кожна тактика та техніка має унікальний ідентифікатор, який слугує для роботи з матрицею.

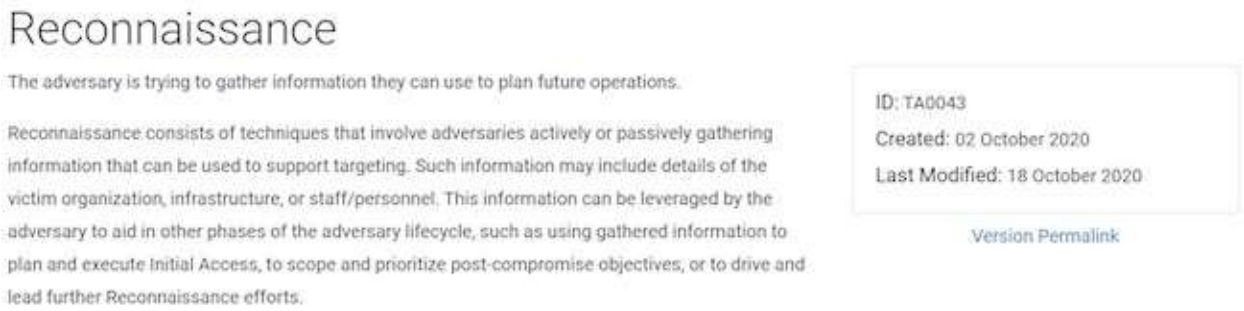



Рис 2.1. Картка тактики TA0043 з описом

Ідентифікатори технік мають вигляд TVVVV.YYY, де VVVV — цифрове позначення номера техніки, а YYY — цифрове позначення підтехніки. Наприклад, T1055.012 "Впровадження в порожній процес" відноситься до техніки T1055 "Впровадження коду в процеси".


Рис 2.2. Картка техніки T1055.012 з описом

Для кожної техніки та підтехніки на сайті MITRE є детальний опис принципу її використання зловмисниками та програм, що застосовуються для цього, названі методи зниження ризику та способи відстеження спроб її реалізації.

## Procedure Examples

| ID | Name | Description |
|---|---|---|
| S0331 | Agent Tesla | Agent Tesla has used process hollowing to create and manipulate processes through sections of unmapped memory by reallocating that space with its malicious code.[3] |
| S0373 | Astaroth | Astaroth can create a new process in a suspended state from a targeted legitimate process in order to unmap its memory and replace it with malicious code.[4][5] |
| S0344 | Azorult | Azorult can decrypt the payload into memory, create a new suspended process of itself, then inject a decrypted payload to the new process and resume new process execution.[6] |
| S0128 | BADNEWS | BADNEWS has a command to download an .exe and use process hollowing to inject it into a new process.[7][8] |
| S0234 | Bandook | Bandook has been launched by starting iexplore.exe and replacing it with Bandook's payload.[9][10][11] |
| S0534 | Bazar | Bazar can inject into a target process including Svchost, Explorer, and cmd using process hollowing.[12][13] |
| S0127 | BBSRAT | BBSRAT has been seen loaded into msiexec.exe through process hollowing to hide its execution.[14] |

Рис 2.3. Картка техніки T1055.012 з описом програм, що використовуються для її реалізації

## Mitigations

| ID | Mitigation | Description |
|---|---|---|
| M1040 | Behavior Prevention on Endpoint | Some endpoint security solutions can be configured to block some types of process injection based on common sequences of behavior that occur during the injection process. |

Рис 2.4. Схема роботи TIP. Заходи, що рекомендуються для зниження ризику використання техніки T1055.012

## Detection

| ID | Data Source | Data Component | Detects |
|---|---|---|---|
| DS0009 | Process | OS API Execution | Monitoring Windows API calls indicative of the various types of code injection may generate a significant amount of data and may not be directly useful for defense unless collected under specific circumstances for known bad sequences of calls, since benign use of API functions may be common and difficult to distinguish from malicious behavior. Windows API calls such as `CreateRemoteThread`, `SuspendThread`/`SetThreadContext`/`ResumeThread`, and those that can be used to modify memory within another process, such as `VirtualAllocEx`/`WriteProcessMemory`, may be used for this technique.[2] |
| | | Process Access | Monitor for processes being viewed that may inject malicious code into suspended and hollowed processes in order to evade process-based defenses. |
| | | Process Modification | Monitor for changes made to processes that may inject malicious code into suspended and hollowed processes in order to evade process-based defenses. |

Рис 2.5. Заходи, рекомендовані для виявлення техніки T1055.012

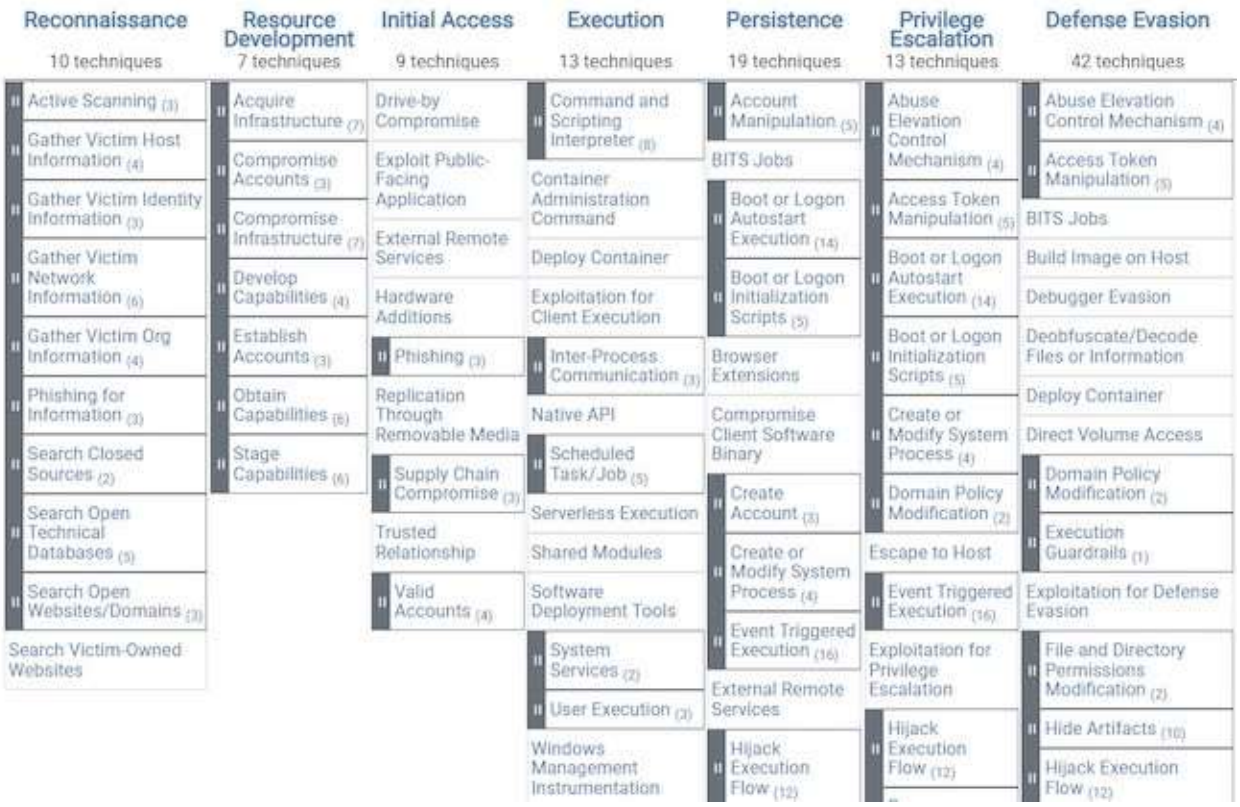



Рисунок 10. Графічне представлення матриці тактик та технік MITRE ATT&CK для сегменту Enterprise

MITRE ATT&CK містить не тільки інформацію про техніки та тактики, а ще низку інших, не менш корисних данних. «Джерела даних» (Data Sources) це розділ в якому міститься інформація про те, які події в галузі безпеки необхідно аналізувати для виявлення спроб використовувати ті чи інші техніки та процедури. Виділено джерела даних для корпоративних та промислових систем, тоді як для мобільних ОС такої інформації в поточній версії матриці немає.

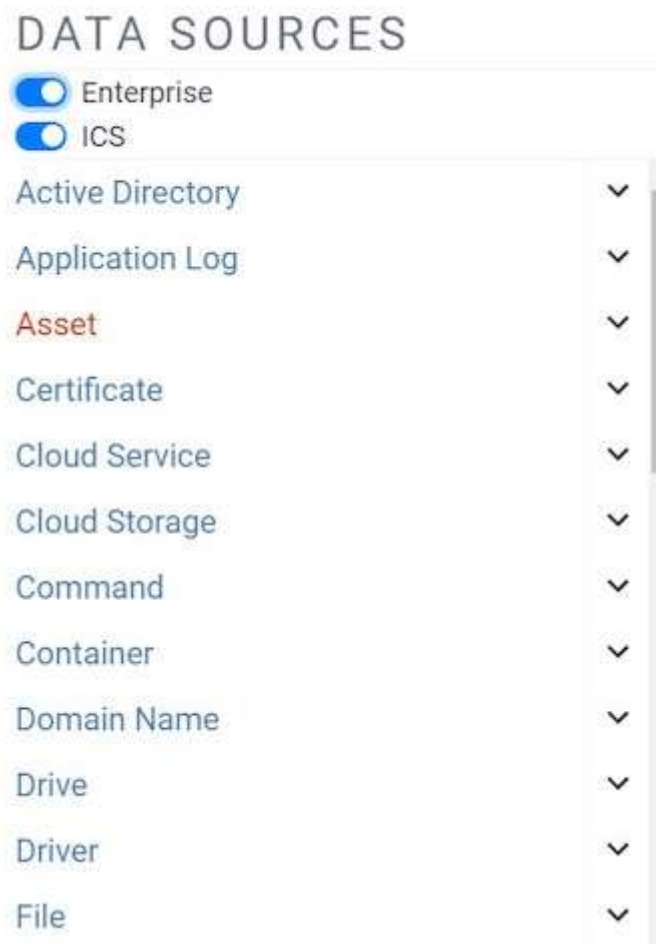



Рис 2.6. Список джерел даних для системи, що захищається

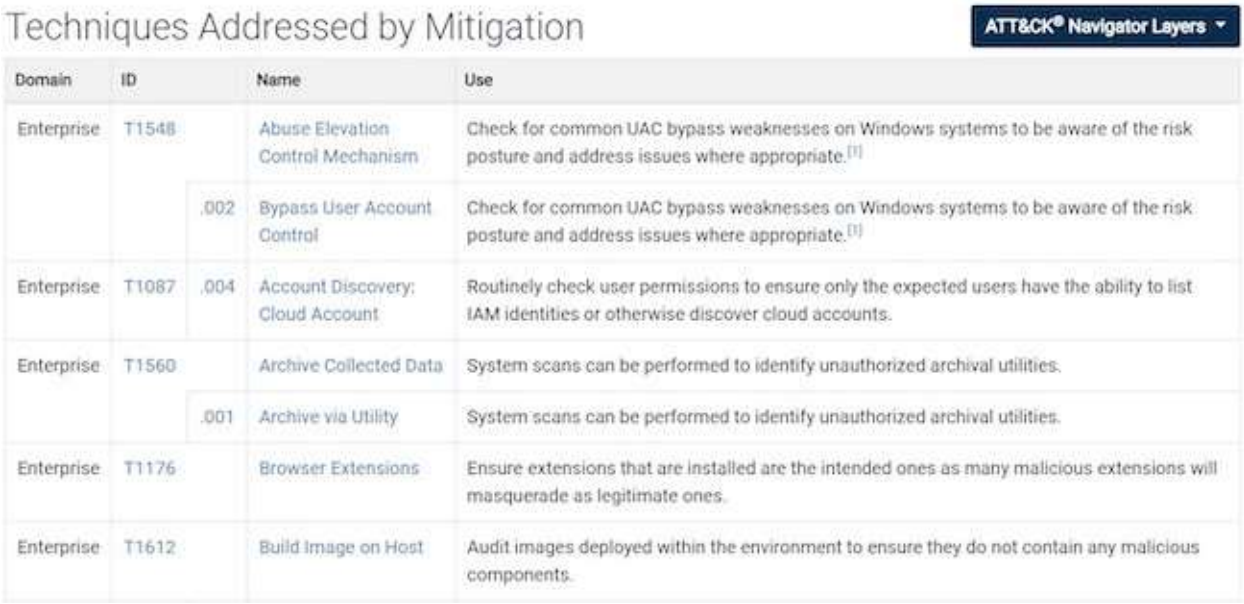
Active Directory: Active Directory Credential Request

A user requested active directory credentials, such as a ticket or token (ex: Windows EID 4769)

| Domain | ID | Name | Detects |
|---|---|---|---|
| Enterprise | T1649 | Steal or Forge Authentication Certificates | Monitor AD CS certificate requests (ex: EID 4886) as well as issued certificates (ex: EID 4887) for abnormal activity, including unexpected certificate enrollments and signs of abuse within certificate attributes (such as abusable EKUs).[2] |
| Enterprise | T1558 | Steal or Forge Kerberos Tickets | Monitor for anomalous Kerberos activity, such as malformed or blank fields in Windows logon/logoff events (Event ID 4624, 4672, 4634), RC4 encryption within ticket granting tickets (TGTs), and ticket granting service (TGS) requests without preceding TGT requests.[3][4][5]Monitor the lifetime of TGT tickets for values that differ from the default domain duration.[6] Monitor for indications of Pass the Ticket being used to move laterally. |
| | .001 | Golden Ticket | Monitor for anomalous Kerberos activity, such as malformed or blank fields in Windows logon/logoff events (Event ID 4769, 4768), RC4 encryption within TGTs, and TGS requests without preceding TGT requests. Monitor the lifetime of TGT tickets for values that differ from the default domain duration. Monitor for indications of Pass the Ticket being used to move laterally. |

Рис 2.7. Варіанти виявлення активності зловмисників під час використання картки DS0026

Опис методів зниження ризиків у MITRE ATT&CK дуже корисним розділом порталу MITRE ATT&CK є інформація про можливість застосування заходів, що компенсують, що мінімізують успішність дій зловмисників. Розділ містить рекомендації для корпоративних, промислових та мобільних систем.



Techniques Addressed by Mitigation

ATT&CK® Navigator Layers

| Domain | ID | | Name | Use |
|---|---|---|---|---|
| Enterprise | T1548 | | Abuse Elevation Control Mechanism | Check for common UAC bypass weaknesses on Windows systems to be aware of the risk posture and address issues where appropriate.[1] |
| | | .002 | Bypass User Account Control | Check for common UAC bypass weaknesses on Windows systems to be aware of the risk posture and address issues where appropriate.[1] |
| Enterprise | T1087 | .004 | Account Discovery: Cloud Account | Routinely check user permissions to ensure only the expected users have the ability to list IAM identities or otherwise discover cloud accounts. |
| Enterprise | T1560 | | Archive Collected Data | System scans can be performed to identify unauthorized archival utilities. |
| | | .001 | Archive via Utility | System scans can be performed to identify unauthorized archival utilities. |
| Enterprise | T1176 | | Browser Extensions | Ensure extensions that are installed are the intended ones as many malicious extensions will masquerade as legitimate ones. |
| Enterprise | T1612 | | Build Image on Host | Audit images deployed within the environment to ensure they do not contain any malicious components. |

Рис 2.8. Приклад використання заходу «Аудит» для зниження ризику реалізації технік та підтехнік

Опис програмного забезпечення в MITRE ATT&CK Програмне забезпечення - це загальний термін для користувача або комерційного коду, утиліт операційної системи, програм з відкритим вихідним кодом або інших інструментів, що використовуються для реалізації поведінки, змодельованої в матриці. Деякі екземпляри програмного забезпечення мають кілька імен, оскільки різні організації відстежують один і той же набір програмного забезпечення під різними іменами. Упорядники матриці оперують двома термінами в описах програмного забезпечення. Перший із них — «інструмент»: програми, які зазвичай не зустрічаються в корпоративних системах або доступні як частина ОС, яка вже є в середовищі. Це можуть бути, наприклад, PsExec, Metasploit, Mimikatz, а також утиліти Windows, такі як Net, Netstat, Tasklist і т. д. для використання зловмисниками. Це може бути, наприклад, PlugX, CHOPSTICK і т.д. Картка шкідливої програми має ідентифікатор

типу «SXXXX», де XXXX — наданий програмному забезпеченню номер. Як приклад розглянемо широко і сумнозвісний Stuxnet, використаний проти ядерної програми Ірану в 2009 р.


Рис 2.9. Опис Stuxnet у MITRE ATT&CK

Опис кампаній у MITRE ATT&CK У MITRE ATT&CK термін «кампанія» використовується для опису будь-якої сукупності дій із вторгнення, проведених із загальними цілями та завданнями протягом певного інтервалу часу. Інформація про кампанію включає опис використовуваних кіберзлочинцями методів і програм. Картка кампанії має ідентифікатор типу «CXXXX», де XXXX — наданий номер.


Рис 2.10. Опис кампанії Night Dragon

Практичне використання MITRE ATT&CK в QRadar Use Case Manager є безцінним джерелом знань для фахівців з інформаційної безпеки, тому що містить багато корисних відомостей, що дозволяють підвищити рівень захищеності інфраструктури. Однак єдиного варіанта її використання немає — все залежить від людських і технічних ресурсів. Розглянемо деякі з варіантів застосування матриці практично. Першим варіантом є всебічне моделювання можливостей проникнення в

інфраструктуру організації, починаючи з етапу розвідки та закінчуючи впливом. Поступово перебираючи всі можливі техніки та підтехніки, можна залишити ті, що є валідними для діючої інфраструктури, і далі вести діяльність щодо зниження ризиків впливу на неї. Цей варіант передбачає скрупульозну роботу та великі трудовитрати, проте в результаті жодні з векторів атак не залишаться поза увагою. Для самостійного моделювання MITRE розробила окремий інструмент – MITRE ATT&CK Navigator . З його допомогою можна визначити вектори атак, які можливі для існуючої архітектури при використанні якої можна значно знизити ймовірність хакерської атаки або помітно ускладнити її розвиток. Матриця затребувана і актуальна: дослідники співвідносять з нею результати своєї роботи, а виробники засобів захисту прагнуть демонструвати ефективність своїх рішень через охоплення описаних у MITRE ATT&CK технік. В QRadar Use Case Manager все налаштовано для використання цих безцінних знань в автоматичному режимі з мінімальним втручання в роботу всі сценарії, моделі відпрацьовані ідеально інженерами з IBM.

## 2.2. Аналіз найбільш популярних рішень для виявлення загроз корпоративній інформаційній системі

В цій роботі розглянуто як основну систему Qradar Use case manager, але завжди треба розглядати інші варіанти, тому що сама безпека це мати декілька можливих рішень які ви можете використати, бо основою будь якої захищеної системи є децентралізована система безпеки де все залежить не тільки від одного забезпечення. Компанії, корпорації мають мати в своєму арсеналі декілька Siem щоб можна було в декілька кліків переключитись на інше ядро ІТС і активувати іншу систему безпеки.

Тому в цій роботі ми також розглянемо інші актуальні на сьогоднішній день системи виявлення вразливостей на базі популярних SIEM.

| Capability | Log Rhythm | Splunk | McAfee Nitro | IBM QRadar | HP ArcSight |
|---|---|---|---|---|---|
| Real-time Security Monitoring | 4.0 | 3.4 | 3.5 | 4.0 | 4.1 |
| Threat Intelligence | 3.5 | 3.5 | 3.7 | 4.0 | 4.0 |
| Behavior Profiling | 3.8 | 3.7 | 3.4 | 3.8 | 4.0 |
| Data & End User Monitoring | 4.1 | 3.5 | 3.7 | 3.5 | 3.5 |
| Application Monitoring | 3.6 | 3.7 | 4.0 | 4.0 | 3.8 |
| Analytics | 3.6 | 4.2 | 3.7 | 3.9 | 3.7 |
| Log Management & Reporting | 3.5 | 3.9 | 3.5 | 3.6 | 3.8 |
| Deployment & Support Simplicity | 4.0 | 3.1 | 3.5 | 4.0 | 3.3 |
| **Total (Weighted Score)** | **30.1** | **29.0** | **29.0** | **30.8** | **30.2** |

Рис 2.11. InfoSec Nirvana рейтинг 2022


Рис 2.12. Gartner Magic Quadrant 2022

Інформація станом на зараз, зараз найактуальніші Use Case в 4 виробників, вони організували власні майданчики для публікації Use Case'ів. Також у більшості виробників є внутрішній форум для обміну інформацією та пошуку рішень проблем, що виникають.

*HPE ArcSight Marketplace - Є платні та безкоштовні. Якщо не застосовувати додаткову фільтрацію, то на сайті сумарно 300+ Use Case'ів.*

*IBM Security App Exchange - Завантаження безкоштовно. Use Case, розроблені як самим IBM, так і партнерами.*

*LogRhythm - Поки що мало Use Case'ів, але розвивають це направлення*

*Splunk - Підрозділ "Security, Fraud and Compliance" містить багато актуальних програм. Але якщо відфільтрувати тільки програми (а не аддони, хоча вони теж важливі) і вказати версію продукту 6.0 і вище - сумарна кількість зменшується до приблизно 300 Use Case'ів.*

Також важливим фактором вибору SIEM системи є якісна можливість інтеграції саме у вашій країні та вашій компанії. Є багато вендорів в яких відсутні якісні можливості інтеграції через компанії інтегратори. Тому ми порівняли всі SIEM системи через призму інтеграції саме в Україні використавши найпопулярніших інтеграторів України, отримуємо такі данні:

| SIEM<br><br>Інтегратор | QRadar | ArcSight | Splunk |
|---|---|---|---|
| Active Audit Agency | - | - | Reseller |
| Betta Security | - | - | Reseller |
| BMS Consulting | Business partner | Gold partner | - |
| CBS Group | Business partner | - | - |
| Center of Systrem Integration | - | Business partner | - |
| COMPAREX Ukraine | Business partner | - | - |
| Comsec | - | - | Reseller |
| CS Integra | - | Business partner | - |
| IBPM | Business partner | - | - |
| ICSystems | - | Business partner | - |
| Integrity Vision | Business partner | - | - |
| ISSP | - | Silver partner. Engineer certified | - |
| IT for Business (Supportio) | - | Business partner | - |
| IT-Integrator (Incom) | Business partner | - | - |
| LanTec | - | Platinum partner | - |
| SI BIS | Business partner | - | - |
| SI Center | - | Business partner | - |
| Spezvuzavtomatika | - | Business partner | - |
| SPro | Business partner | - | - |
| SVIT IT | Business partner | Gold партнер. Engineer certified | - |
| System Integration Service | Business partner | - | - |

Рис 2.13. Порівння можливості інтеграції різних SIEM в Україні

Порівнявши результати можемо дійти висновку, що Qradar має найширші можливості інтеграції серед обраних вендорів на Українському ринку. Це свідчить про те що Qradar якісна система яку можливо якісно інтегрувати у більшості компаній.

# 3 ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ЗАГРОЗ КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

## 3.1. Варіант системи виявлення загроз корпоративній інформаційній системі на базі рішення QRadar Use Case Manager

Практичне використання QRadar Use Case Manager є необхідним для якісного виявлення загроз корпоративній інформаційній системі. З початку QRadar Use Case Manager вже оптимально налаштований для вашої системи. Також можна скористуватися підказками щоб впевнитися в правильному налаштуванні вашої системи на точне виявлення атак, зробити зміни щоб не було хибних спрацювань і щоб загрози ідентифікувались вірно.

Створювати нові правила зручно, можливо переглядати вже наявні через фільтри. Створювати звіти також зручно на основі вже розроблених шаблонів, дуже багато різних складових є для створення звітів щоб вони були максимально зручні і корсині.

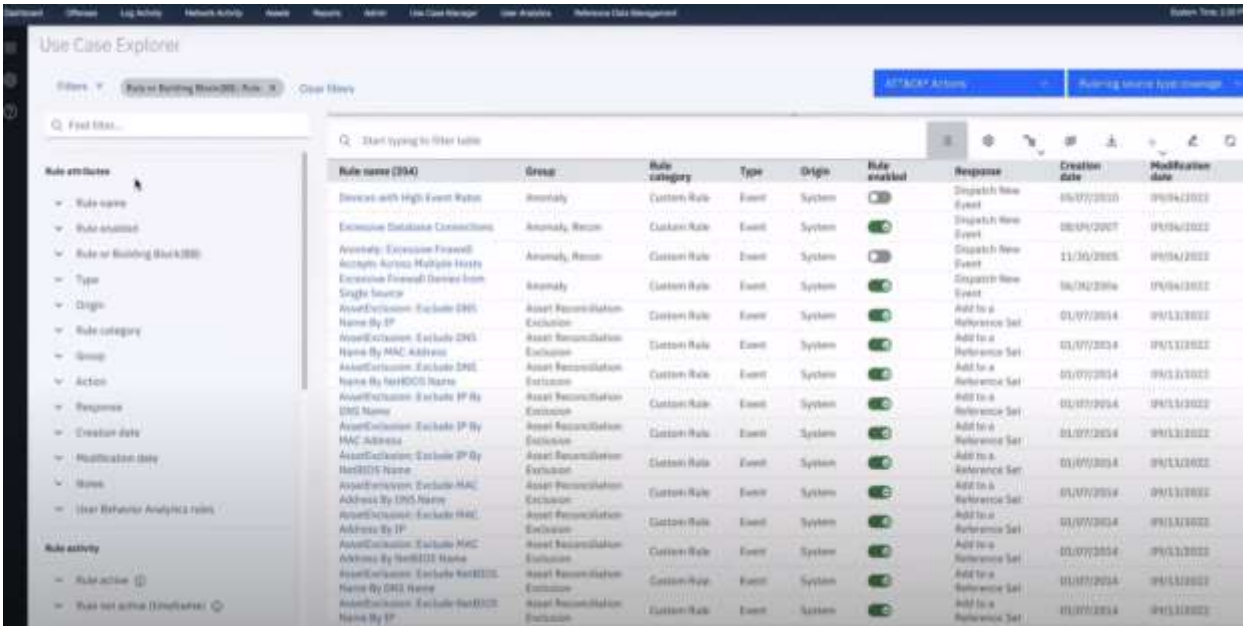



Рис 3.1. Налаштування правил в QRadar Use Case Manager

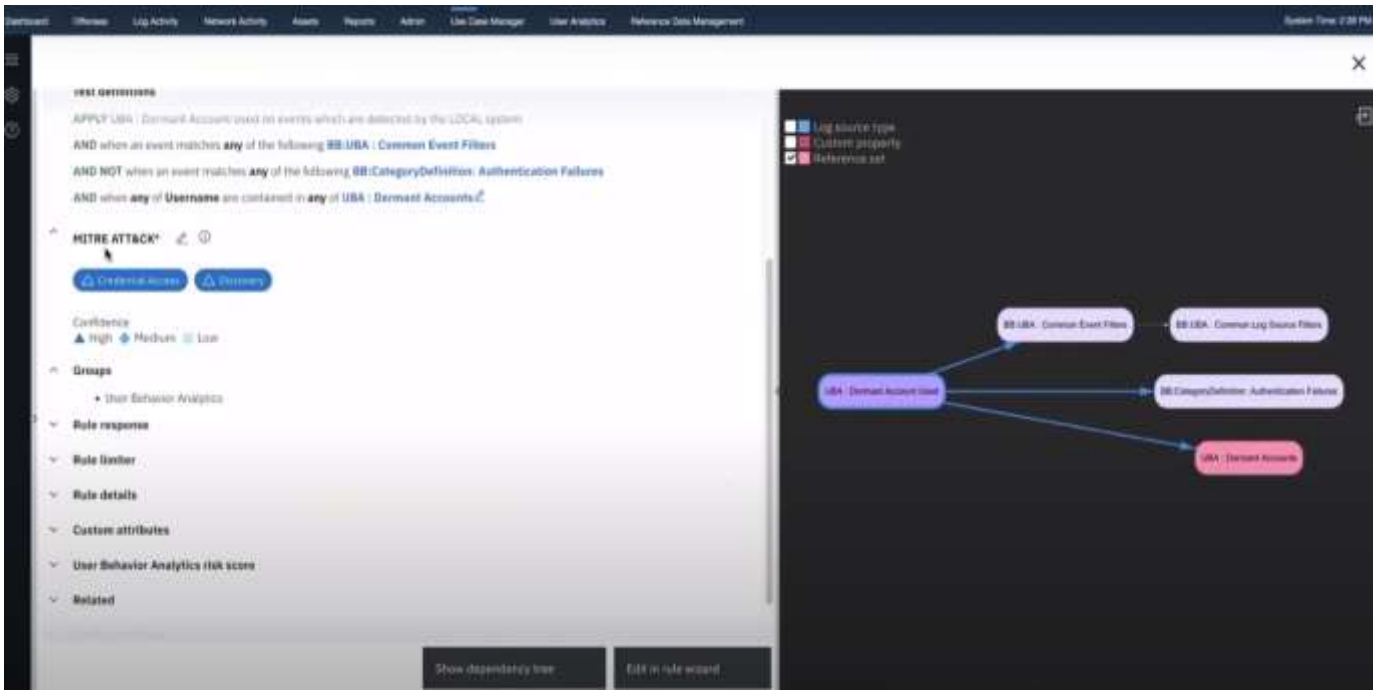



Рис 3.2. Деталі роботи правила QRadar Use Case Manager

З усіх запропонованих правил нам треба ввімкнути нам потрібні, а потім їх налаштувати, дуже важливим при цьому є пункт MITER ATT&CK щоб створити декілька методів можливої атаки.

Дуже важливим аспектом є оптимізація наших правил для зменшення хибних спрацювань, з самого початку їх буде багато але з часом їх кількість маю прямувати до нуля.

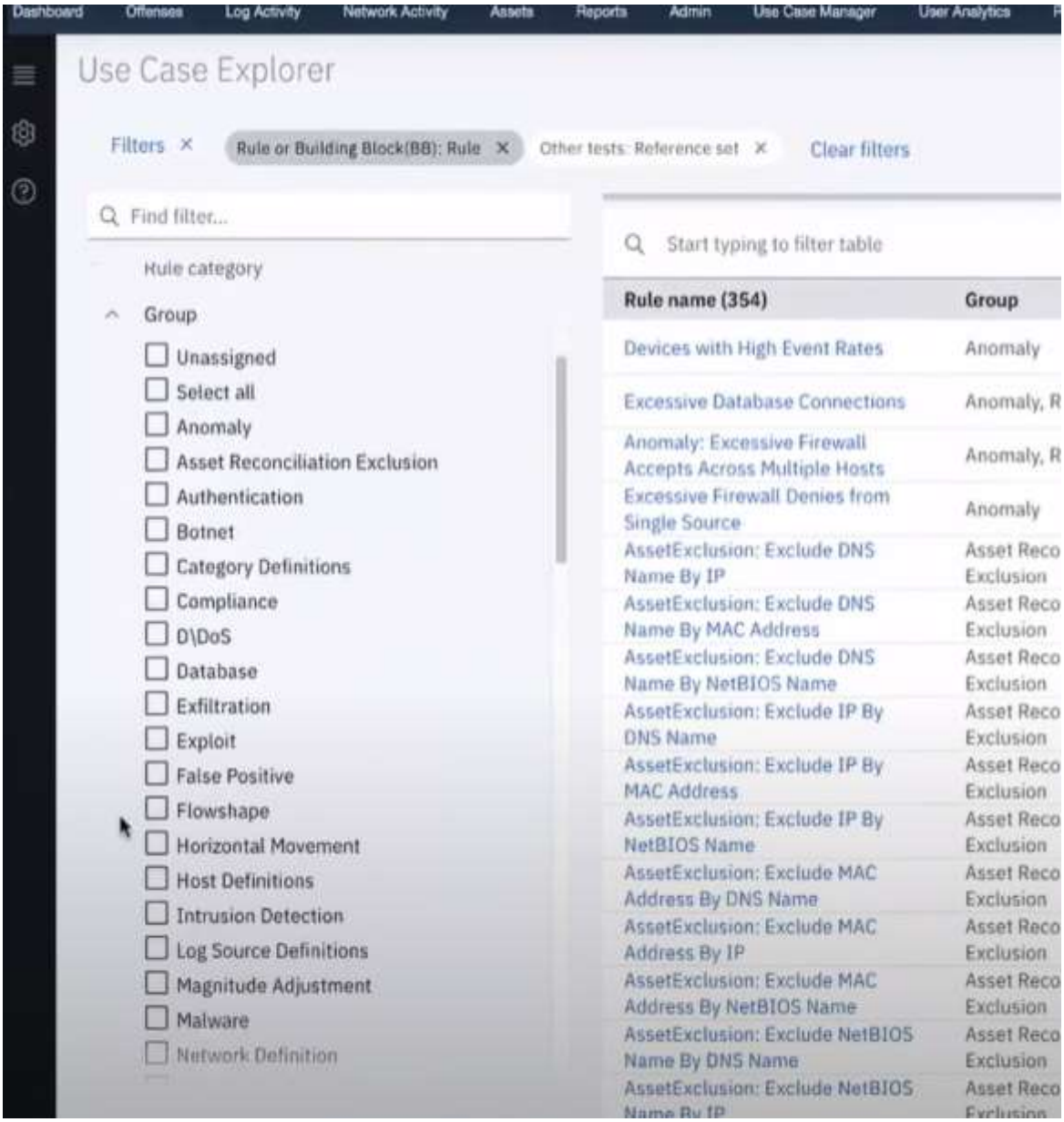



Рис 3.3. Фільтр по групам для правил QRadar Use Case Manager

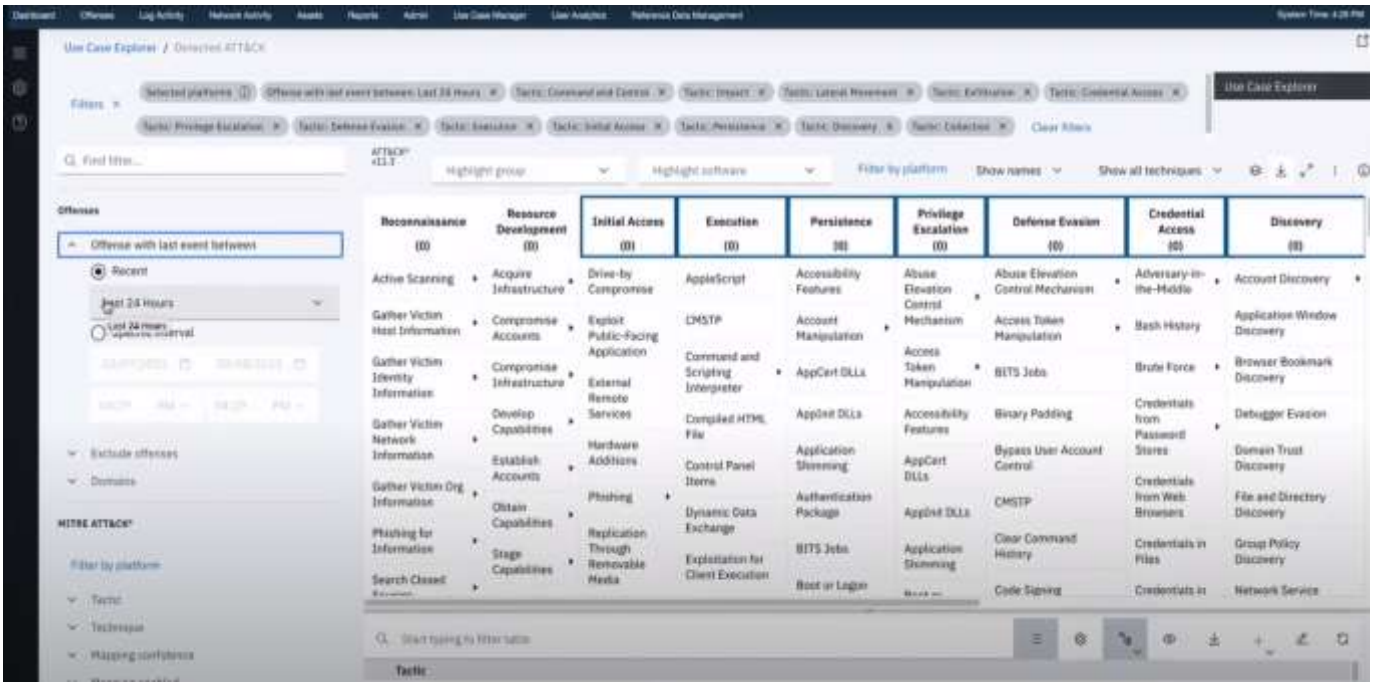



Рис 3.4. Деталі роботи правила і спрацювання за 24 години QRadar Use Case Manager

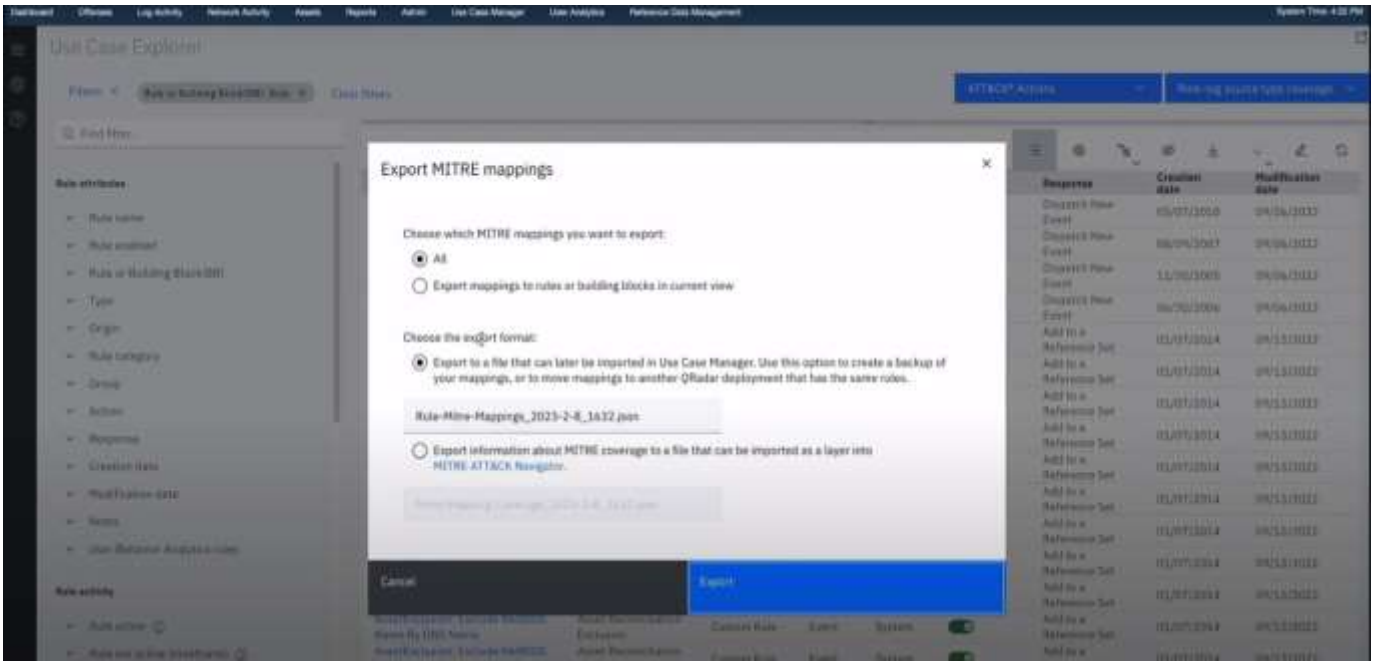



Рис 3.5. Експорт тактик для певного правила QRadar Use Case Manager


Рис 3.6. Панель логів правил QRadar Use Case Manager

Ми також можемо оптимізувати наші правила шляхом експорту тактик не хибних спрацювань, щоб знизити кількість їх. Можемо проводити глибоку візуалізовану аналітику щодо наших правил та через деякий час навіть відслідковувати певні тенденції вразливостей в нашій системі.

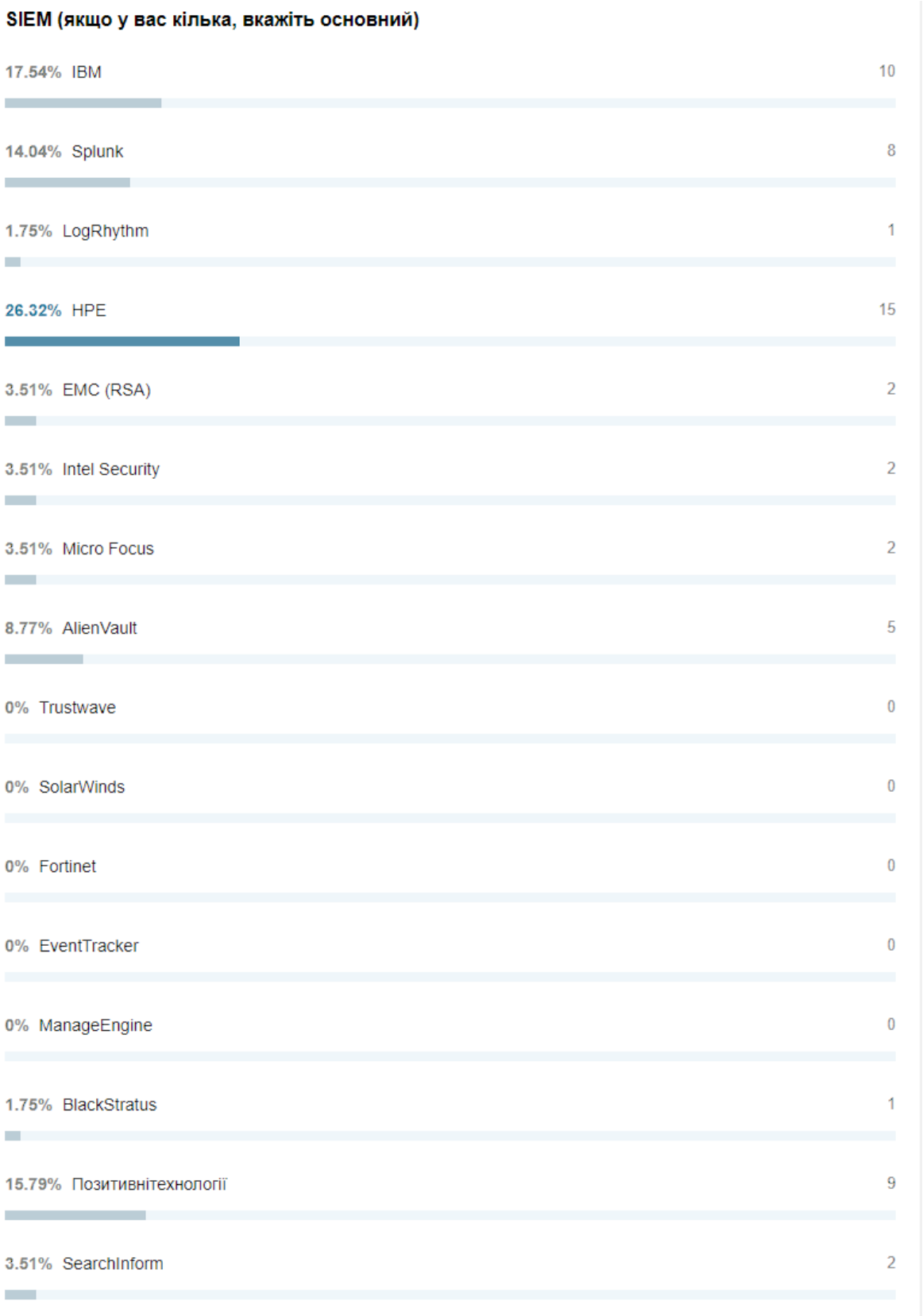



Рис 3.7. Найпопулярніша SIEM серед представників компаній які обирали SIEM.

## 3.2. Рекомендації щодо підвищення можливостей виявлення загроз корпоративній інформаційній системі

Для підвищення можливостей виявлення загроз у корпоративних інформаційних системах існує дуже багато методів та засобів проте ми розберемо найбільш ефективні виходячи з мого власного досвіду. На 99% відсотків компанії, корпорації, бізнес використовують SIEM системи в яких є Use Case, і в мережі інтернет і у вендорів SIEM систем ми маємо безліч прописаних сценаріїв, але нові загрози постають перед нами кожен день, тому будь який інженер має вміти прописувати Use Case-и. Для своєчасної відповіді сучасним загрозам прописання таких сценаріїв є необхідністю, тому я підготував основні рекомендації по створенню таких Use Case-ів.

Рекомендації щодо самостійного написання Use Case'ів

Методологія розробки Use Case'ів необхідно підійти до завдання як до повноцінного міні-проекту:

- Чітко визначитися з вирішуваним завданням та її джерелом (це може бути вимога бізнесу, необхідність відповідати стандартам та регламентам індустрії захисту даних тощо).
- Визначити межі проекту (тобто конкретну ділянку IT-інфраструктури, що захищається).
- Після цього виявити можливі джерела подій, обробка яких дозволить реалізувати працюючий Use Case. Це можуть бути логи з пристроїв, журнали подій, конфігураційні установки.
- Перевірити, що джерело справно постачає всі необхідні дані - інакше коректно розроблений Use Case не зможе ефективно працювати (не спрацьовуватиме, або навпаки видаватиме False Positive - помилкові спрацьовування).
- Нарешті розпочати розробку Use Case'а.

- Встановити та тестувати, підлаштовуючи логіку та пороги спрацьовування.
- Коли Use Case вже перевірено та встановлено у продуктив, важливо правильно налаштувати реакцію на його спрацювання: чи достатньо просто виводити дані на дашборд, чи потрібно сповіщення по SMS/email, або навіть автоматично запускати зміну конфігурації підлеглих пристроїв (наприклад, IBM декларує, що її SIEM зможе змінити правила IPS/Firewall'a).

Коли, все працює це добре! Але робота на цьому не завершена — необхідно обслуговування (maintenance) розробленого міні-продукту: періодично перевіряти, чи надходять дані для обробки, чи не змінився їх формат, доопрацьовувати сам Use Case під топологію IT-інфраструктури і потреби Бізнесу, що змінюється

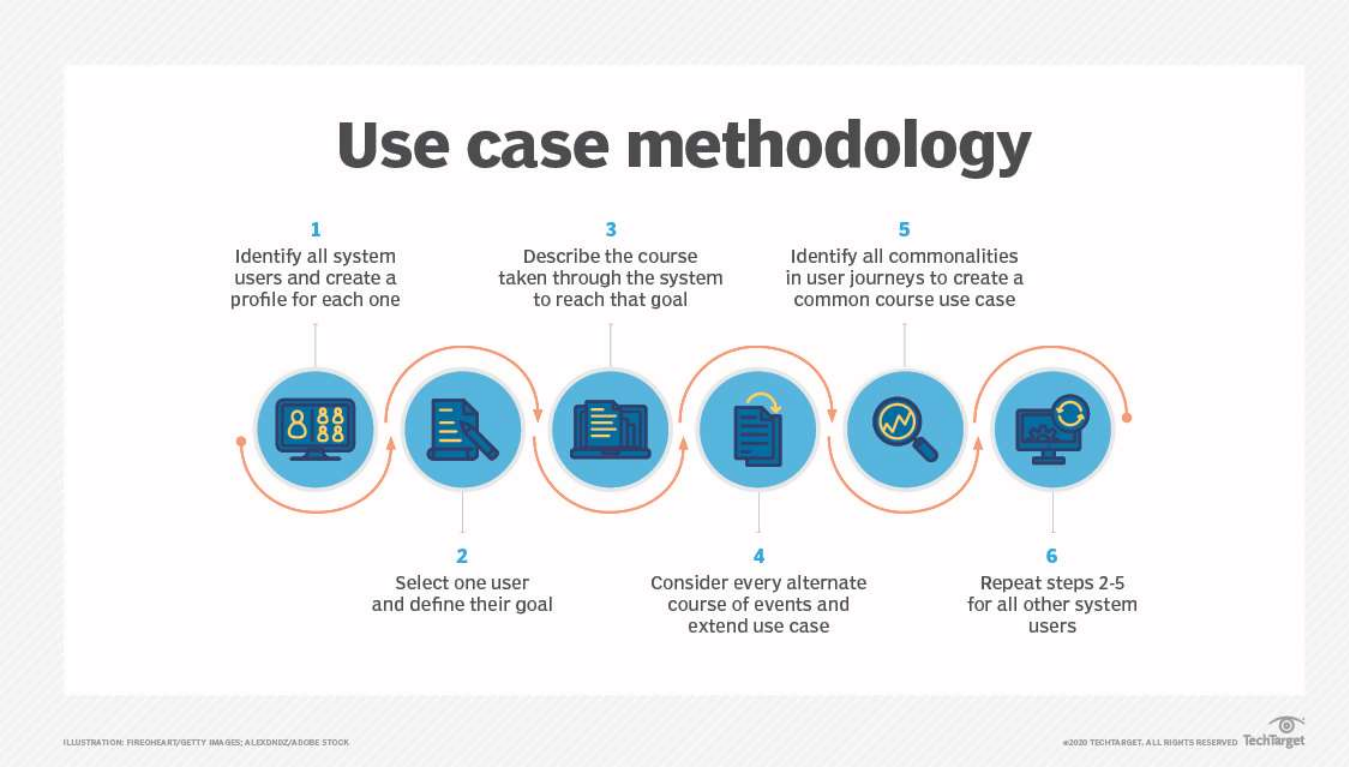



Рис 3.8. Use case методологія створення

Під час написання сценарію використання розробники можуть використовувати схему послідовності, яка показує, як об’єкти реагують на часовій шкалі, щоб моделювати взаємодії між об’єктами в одному випадку використання. Діаграми послідовності дозволяють розробникам бачити, як кожна частина системи взаємодіє з

іншими для виконання певної функції, а також порядок, у якому відбувається ця взаємодія.

Не завжди є можливість оплачувати дорого вартісне ПЗ SIEM-систем, або рівень захисту настільки високий що використання не власної SIEM, може дуже нашкодити це наприклад оборонна промисловість, державний апарат, силові структури та інші державні структури та апарати.

Також дуже часто є проблема того що у вашій компанії, бізнесі, корпорації де ви працюєте, є необхідність в тих функціях або є певні особливості які не дозволяють вам використовувати загальні рішення. Інтегратори не завжди можуть інтегрувати вже готові SIEM системи саме під вашу компанію, якісно та з урахуваннях ваших особливостей та потреб. І в такій ситуації не залишається варіантів як зробити своє власне рішення з потреб та особливостей компанії для якої таке рішення створюється. Для розроблення власної SIEM системи згадаємо її фунції та основне завдання.

Основне завдання SIEM системи – аналізувати події, що реєструються в інфраструктурі, що надходять від різних джерел, і виявляти атаки/сценарії атак/підозрілі дії/відхилення від норми, формуючи при необхідності відповідні інциденти безпеки.

Базові можливості системи SIEM повинні забезпечувати вирішення наступних завдань:

- збирання та зберігання подій безпеки, що надходять;
- обробка та аналіз зареєстрованих подій безпеки;
- виявлення атак та порушень політик безпеки у реальному часі (близькому до реального часу);
- виявлення та розбір інцидентів безпеки;
- формування звітів.

Крім того, до сучасних рішень класу SIEM висуваються додаткові вимоги з метою забезпечення реалізації наступних функціональних можливостей:

- оцінка захищеності ресурсів контрольованої системи;

- перевірка відповідності системи управління ІБ існуючим вимогам та нормам;
- управління ризиками ІБ та ін.

Функціональна модель системи SIEM має такі функціональні підсистеми: збирання даних, попередньої обробки, зберігання, аналізу, подання. Узагальнена послідовність обробки подій безпеки у рішеннях SIEM пояснюється малюнком:

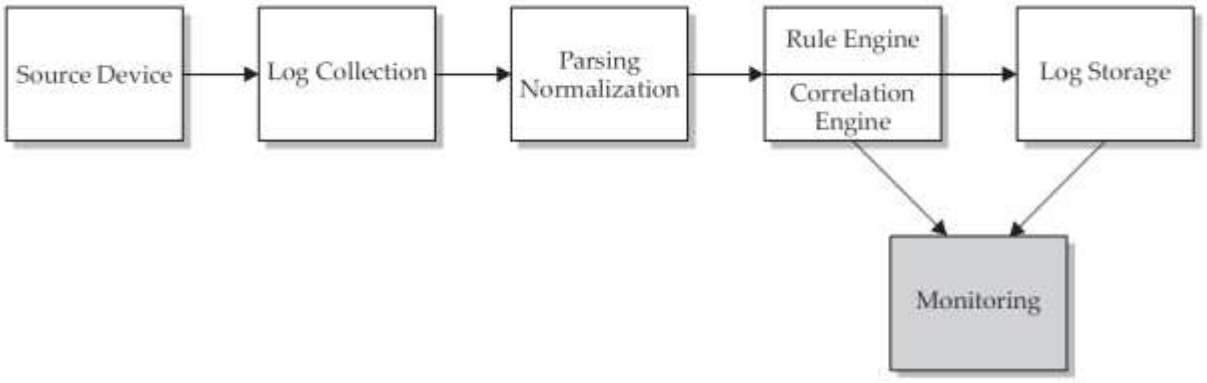



Рис 3.9. Функціональна модель системи SIEM

Далі ми розглянемол приклад розробки власної SIEM системи. У прикладі моделюється спрощений сценарій атаки типу «перебір пароля» щодо нашого веб-додатку. Основне завдання SIEM системи, що розробляється, - сповістити адміністратора безпеки про спробу реалізації такої атаки.

Для створення нашої власної SIEM системи, використовувалися open-source рішення та власні скрипти, додатки, тулзи, а також вже створені однодумцями на GitHUB написані на PHP та C#. Архітектура віртуальної системи представлена на рисунку.

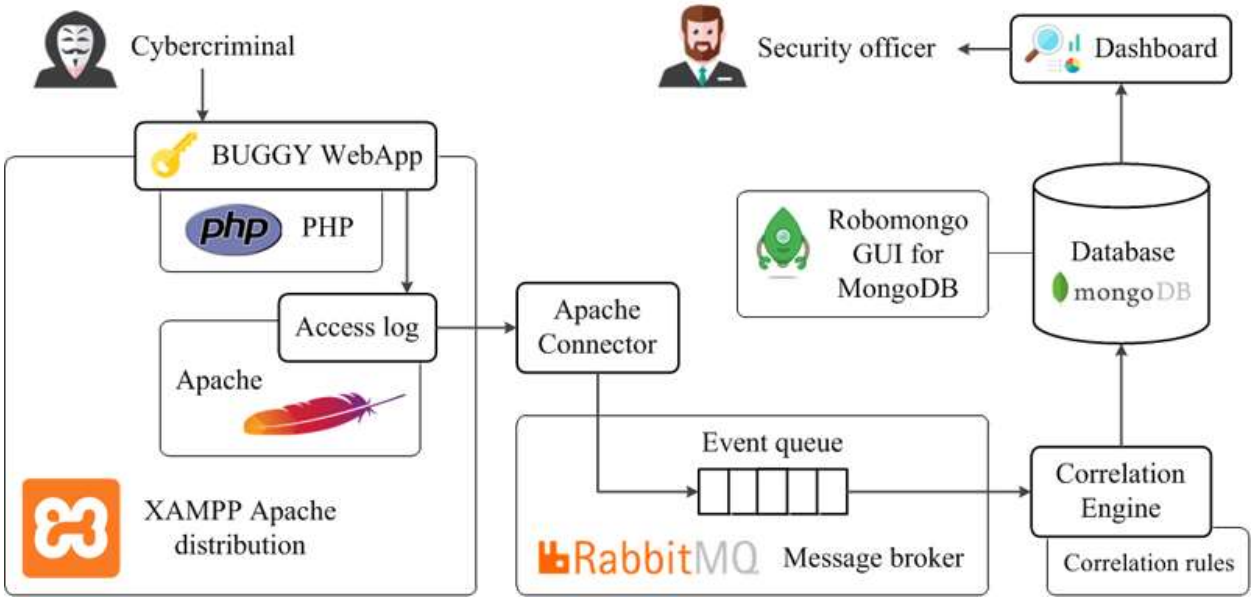



Рис 3.10. Архітектура SIEM

1. Організація тестового оточення.
    1.1. Встановлення та налаштування веб-сервера Apache.
    1.2. Встановлення та налаштування сховища даних MongoDB.
    1.3. Встановлення та налаштування брокера повідомлень RabbitMQ.
    1.4. Встановлення та налаштування середовища розробки Visual Studio.
2. Розробка веб-програми Buggy Webapp, що захищається.
3. Розробка конектора для веб-сервера Apache.
4. Розробка ядра кореляції (обробника подій).
    4.1. Оцінка продуктивності сховища даних MongoDB.
    4.2. Формування набору правил кореляції.
    4.3. Реалізація ядра кореляції.
5. Розробка консолі адміністратора безпеки.
6. Перевірка працездатності розробленої SIEM системи.

1.1 Встановлення та налаштування веб-сервера Apache

Як веб-сервер будемо використовувати складання XAMPP for Windows, версія 7.1.9 (Apache 2.4.27 + PHP 7.1.9). Завантажуємо та встановлюємо XAMPP за

допомогою інсталятора, вибираємо папку для встановлення за замовчуванням – «c:\xampp\».

Для перевірки правильності встановлення веб-сервера достатньо відкрити панель керування XAMPP Control Panel та запустити модуль Apache. Після цього у браузері за адресою «http://127.0.0.1/» відкриється вітальна сторінка проекту XAMPP.

Якщо помилок немає, переходимо до наступного пункту.

1.2 Встановлення та налаштування сховища даних MongoDB

Для організації сховища даних пропонується використовувати документну базу даних MongoDB. Основна причина такого вибору – вирішення освітнього завдання та ознайомлення з підходами NoSQL. Крім того, навіть поверхове вивчення комерційних SIEM систем дозволяє зробити висновок про те, що більшість провідних виробників разом із традиційними SQL базами даних у своїх рішеннях застосовують технології NoSQL/NewSQL. Нижче представлена модель однієї відомої комерційної SIEM системи, що підтверджує використання виробником рішень MongoDB та RabbitMQ (брокер повідомлень, що розглядається далі):

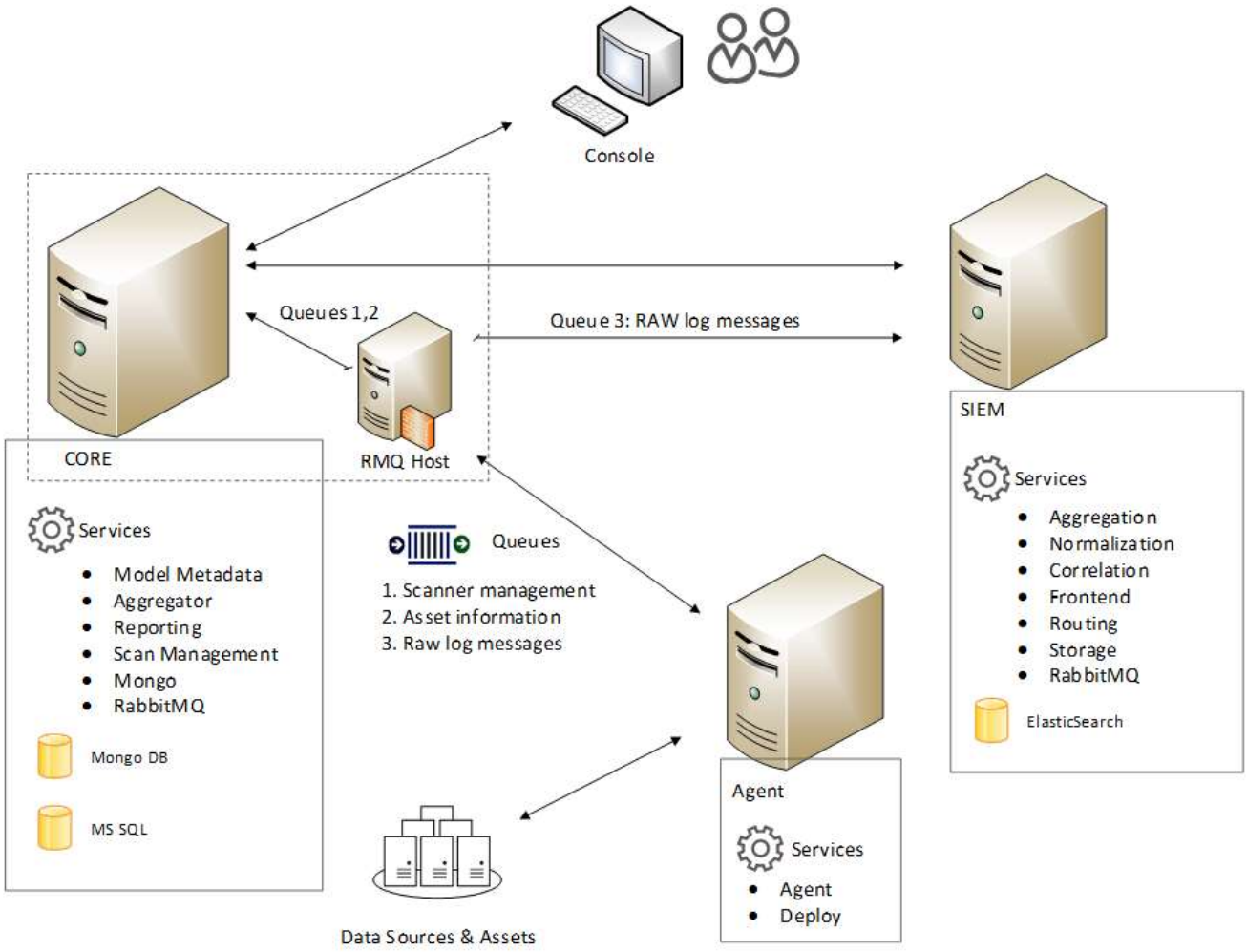



Рис 3.11. Модель комерційної системи SIEM

Завантажуємо з офіційного сайту та встановлюємо інсталяційний пакет MongoDB Community Server. Перевіряємо працездатність сервера, створивши в колекції (collection) test новий документ (document) з полем (field) {a:1}. Спроба знайти документ у колекції має завершитися успіхом.

1.3 Встановлення та налаштування брокера повідомлень RabbitMQ

Для організації обміну даними між компонентами системи будемо використовувати брокер повідомлень RabbitMQ, одне з найпоширеніших рішень подібного класу.

1.4 Встановлення та налаштування середовища розробки Visual Studio

Так склалося, що розробка ядра обробки подій безпеки нашому колективі ведеться на C#. Тому частина прикладів буде на C#.

2. Розробка веб-програми Buggy Webapp, що захищається

Наприклад розробимо просте веб-додаток, що реалізує функцію автентифікації користувача. Надихаємося ідеями мінімалізму в розмітці, верстаємо макет програми з використанням Bootstrap 4. Для реалізації використовуємо мову PHP. Але все залежить від ваших вмінь тому це все індивідуально.

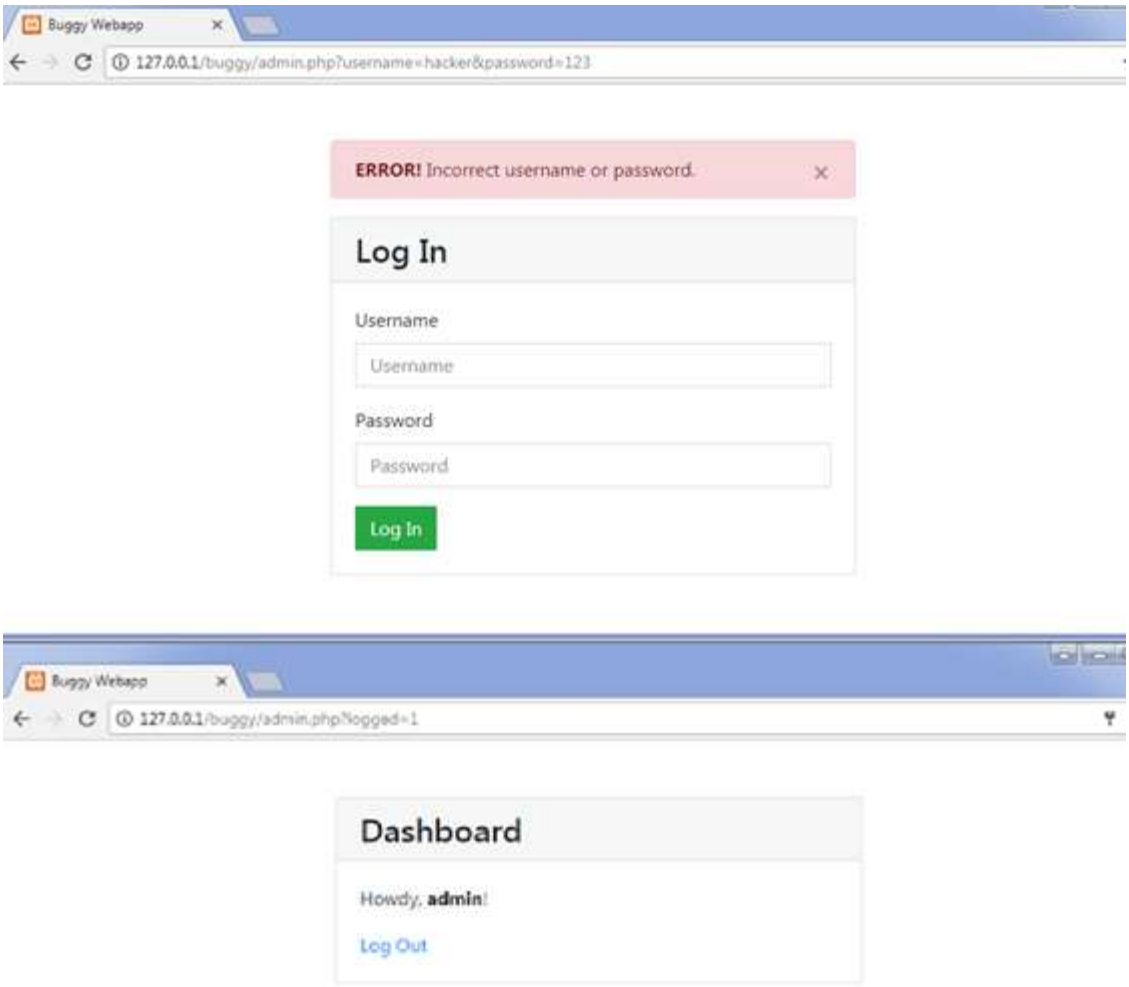



Рис 3.12. Наш веб додаток автентифікації

3. Розробка конектора для веб-сервера Apache

Як відстежити звернення до веб-програми, що захищається, і спробувати виявити підозрілі дії користувачів? Простий та зрозумілий спосіб – переглянути журнал доступу (журнал звернень) веб-сервера.

Розробляємо алгоритм. Опис роботи алгоритму:

- На початковому етапі звертаємося до журналу доступу access.log та запам'ятовуємо розмір файлу.
- Далі в безкінечному циклі з паузою між ітераціями відстежуємо зміни розміру файлу. При збільшенні розміру читаємо з файлу останні додані рядки та передаємо у чергу повідомлень RabbitMQ, запам'ятовуємо новий розмір файлу.
- Файл access.log можна перезаписати. Враховуємо такий випадок (зменшення розміру файлу).

Для складання конектора потрібно підключити до проекту .NET/C# RabbitMQ client library. Найпростіше це зробити, встановивши відповідний пакет NuGet у консолі Package Manager Console середовища розробки Visual Studio

4. Розробка ядра кореляції (обробника подій)

Отже, до цього етапу ми налаштували підсистему збору подій безпеки від одного джерела – веб-сервера Apache. Конектор ApacheConnector відстежує зміни журналу звернень access.log і надсилає останні рядки в чергу брокера повідомлень RabbitMQ.

Наступний етап – розробка ядра кореляції (обробника подій). Але попередньо, як було зазначено раніше, пропонується оцінити швидкість запису та читання зі сховища даних MongoDB. Очікуємо, що цей компонент буде bottleneck системи, що розробляється, і визначить верхню межу продуктивності.

4.1 Оцінка продуктивності сховища даних MongoDB

Тестування продуктивності виконаємо простим способом – спочатку оцінимо швидкість послідовного запису в сховищі (одинокові документи та пакети документів), а потім оцінимо швидкість випадкового читання документа з колекції.

4.2 Формування набору правил кореляції

І ще один відступ. Ядро кореляції під час вступу чергової події безпеки намагається застосувати щодо нього заздалегідь завантажені правила обробки

(правила виявлення залежностей між окремими подіями, правила кореляції). Сформуємо тестовий набір правил, який буде використовуватись далі у прикладі.

```
<group name="web-app">

  <rule id="100000" level="0">
    <match>/buggy/</match>
    <description>Access to BUGGY webapp</description>
  </rule>

  <rule id="100001" level="0">
    <if_sid>100000</if_sid>
    <match>password</match>
    <description>Attempt to login to BUGGY webapp</description>
  </rule>

  <rule id="100002" level="1" frequency="3" timeframe="5">
    <if_matched_sid>100001</if_matched_sid>
    <same_source_ip/>
    <description>Brute force trying to login to BUGGY webapp</description>
  </rule>

</group>
```

Рис 3.13. Наш веб додаток автентифікації

Елемент <rule> описує правило.

Атрибут id елемента <rule> визначає ідентифікатор правила. Ідентифікатори вибираємо з діапазону, рекомендованого проектом OSSEC для «авторських» правил: >=100000.

Атрибут level елементу <rule> визначає рівень важливості правила. Мінімальне значення – 0 (загалом не відображаємо в консолі адміністратора безпеки), максимальне значення – 16.

Елемент <match> задає підрядок для пошуку в рядку повідомлення, що обробляється.

Елемент <description> задає опис правила, яке відображатиметься як оповіщення для адміністратора безпеки.

Випадок спрацьовування такого правила перевіряється просто – якщо підрядок, вказаний в елементі <match>, буде виявлений у рядку повідомлення, що обробляється, ядро кореляції сформує оповіщення безпеки.

Логіка правила 100000 наступна: оповіщати систему безпеки про всі спроби звернення до веб-застосунку Buggy Webapp, що захищається. Для цього відстежується підстрока /buggy/ у всіх зверненнях до веб-сервера. Рівень значущості правила 100000 нульовий, критичність у відстежуваних зверненнях відсутня, спрацьовування правила використовуватимуться для побудови складніших ланцюжків правил.

В описі правила 100001 є новий елемент <if_sid> з ідентифікатором правила 100000, який накладає додаткову умову спрацьовування – необхідно, щоб раніше спрацювало правило 100000.

Логіка правила 100001: якщо рядок, що обробляється, має відношення до доступу до веб-програми, що захищається (попередньо спрацювало правило 100000) і при цьому у зверненні до веб-сервера виявлено підрядок «password» (можливо свідчить про передачу пароля у форму введення імені користувача та пароля) , то сповістити систему безпеки про спробу отримання адміністративного доступу - "Attempt to login to BUGGY webapp".

Правило 100001 дозволяє виявляти залежності між окремими подіями безпеки та коректно може називатися правилом кореляції.

В описі правила 100002 є новий елемент <if_matched_sid> з ідентифікатором правила 100001, який накладає додаткову умову спрацьовування, необхідно, щоб правило 100001 спрацювало не менше 3 разів (атрибут frequency=«3» елемента <rule>) протягом останніх 5 секунд (timeframe=«5»). Набір правил кореляції для прикладу сформований, переходимо до безпосередньої реалізації обробника подій. Наприкінці прикладу виконаємо покрокове налагодження ядра кореляції і перевіримо, як застосовуються правила кореляції до подій безпеки, що надходять, і які оповіщення при цьому формуються. Логіка правила 100002: якщо протягом останніх 5 секунд з однієї і тієї ж адреси зафіксовано безліч спроб (3 і більше) отримання доступу до веб-

додатку, що захищається, то сформувати оповіщення з більш високим рівнем значущості level=«1» про спробу підбору пароля доступу – «Brute force trying to login to BUGGY webapp».

Порожній елемент <same_source_ip/> вказує на те, що при підрахунку спрацьовувань правила, заданого елементом <if_matched_sid>, враховуються лише спрацьовування з відповідними IP-адресами джерела.

4.3 Реалізація ядра кореляції

Програмна реалізація ядра кореляції є найскладнішою і об'ємною частиною прикладу, по суті визначаючи всю логіку обробки подій безпеки SIEM системи, що розробляється.

У загальному вигляді логіка роботи ядра кореляції описується так:

- Ядро кореляції "слухає" чергу повідомлень AirSIEM_ConnectorQueue.
- При надходженні чергового повідомлення (події) ядро намагається застосувати щодо нього заздалегідь завантажені правила обробки подій (правила кореляції).
- У разі застосування одного з правил до дії, що надійшла, ядро при необхідності формує інцидент безпеки і зберігає його в колекції alerts сховища даних MongoDB.

5. Розробка консолі адміністратора безпеки

Для зручності роботи адміністратора безпеки передбачимо відповідне рішення – консоль керування. Функціонал консолі обмежимо переглядом сформованих інцидентів безпеки, варіант реалізації – веб-додаток PHP. Щоб PHP міг взаємодіяти з MongoDB, потрібно виконати дві дії: до інтерпретатора PHP підключити відповідне розширення, а до веб-додатку – відповідну бібліотеку.

5.1 Підключення розширення php_mongodb.dll до веб-сервера

Згадаємо, що ми використовуємо як веб-сервер збірку XAMPP for Windows. За умовчанням інтерпретатор PHP не знає про існування сховища MongoDB, виправити

це можна інсталяцією драйвера MongoDB PHP Driver on Windows. Інсталюємо драйвер Windows, PHP Version 7.1, thread safe, x86.

5.2 Підключення до веб-застосунку бібліотеки MongoDB PHP Library

Далі необхідно підключити до проекту консолі адміністратора бібліотеку MongoDB PHP Library. Вивчаємо офіційну документацію. У посібнику рекомендується найпростіший спосіб – за допомогою Composer.

6. Перевірка працездатності розробленої SIEM системи

Отже, розробка системи SIEM завершена. На заключному етапі ми маємо виконати покрокове налагодження ядра кореляції та переконатися у правильності роботи всього рішення в цілому. Нагадаємо основне завдання системи, що розробляється - сповістити адміністратора безпеки про спробу реалізації сценарію атаки типу «перебір пароля» щодо веб-програми, що захищається.

Відкриваємо у браузері консоль адміністратора безпеки за адресою: http://127.0.0.1/console/index.php. Якщо всі компоненти SIEM системи налаштовані правильно, після виконання тестового сценарію вікно консолі повинне мати приблизний вигляд:

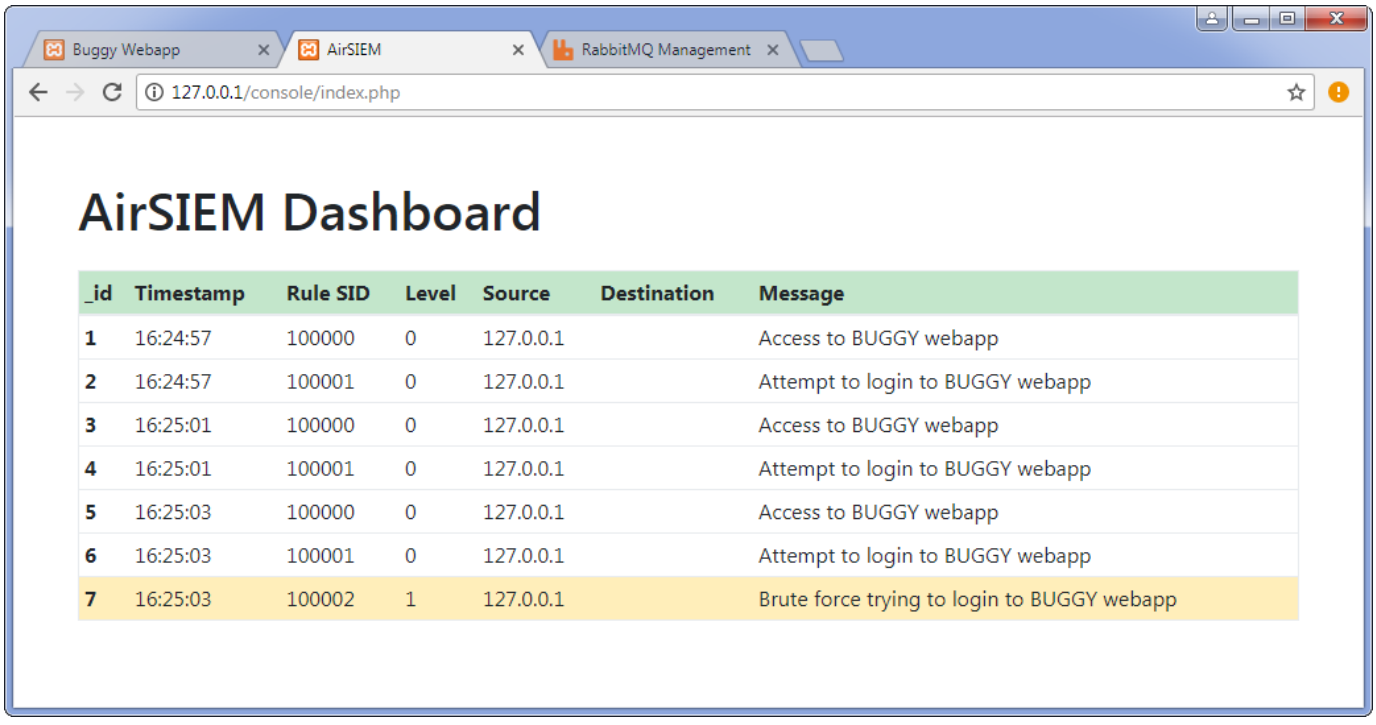



Рис 3.14. Результат атаки перебір паролю

# ВИСНОВОК

В цій роботі було проаналізовано проблему виявлення загроз в корпоративних інформаційних системах, динаміку появи нових загроз. Зловмисники з кожним днем створюють все більш небезпечні загрози, використовують нові методи та тактики щоб проникнути до корпоративних інформаційних систем і їх ціль одна це збагачення. Також не варто не забувати про загрози з середини, контроль співробітників є важливою частино безпеки.

Було розглянуто та проаналізовано QRadar Use Case Manager, порівняли його з конкурентами оцінили можливості в середині системи. По функціональній частині він має найбільше MITRE ATT&CK методів, тактик та сценаріїв що в свою чергу покриває більше вразливостей, широкі можливості застосування правил, оптимізація від хибних спрацювань, і все це з максимальною кількістю функцій

Також що важливо розглянули питання інтеграції загалом SIEM систем в Україні. Порівняли популярні SIEM в таблиці. Лідером серед усіх вибраних нами SIEM систем виявився QRadar Use Case Manager, він має найкращі можливості інтеграції в Україіні. Опитування серед інженерів ІБ свідчить про те що в Україні станом на зараз найбільше компаній обирають саме QRadar Use Case Manager.

В роботі було розглянуто важливе питання самостійного написання Use Case, та дані практичні інструкції та рекомендації щодо їх написання.

В роботі була розроблена своя SIEM система, та дані практичні та методичні рекомендації щодо розроблення своєї системи, а також підхід до створення таких систем.

# ПЕРЕЛІК ПОСИЛАНЬ


1. Загрози інформаційної безпеки // Wikipedia: The free encyclopedia. – San Fracisco: Wikimedia Foundation, 2014. [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/%D0%97%D0%B0%D0%B3%D1%80%D0%BE%D0%B7%D0%B8_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE%D1%97_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8

2. QRadar Use Case Manager // IBM X-force[Електронний ресурс] – Режим доступу: – https://exchange.xforce.ibmcloud.com/hub/extension/bf01ee398bde8e5866fe51d0e1ee684a

3. QRadar Use Case Manager documentation [Електронний ресурс] – Режим доступу: https://www.ibm.com/docs/ru/qradar-common?topic=apps-qradar-use-case-manager-app

4. Securitymedia Електронний ресурс] – Режим доступу: https://securitymedia.org/analytics/obzor-instrumentov-dlya-soc-tsentrov.html

5. Habr [Електронний ресурс] – Режим доступу: https://habr.com/ru/articles/316496/

6. Sprintzeal [Електронний ресурс] – Режим доступу: https://www.sprintzeal.com/blog/top-cybersecurity-threats

7. Spice works [Електронний ресурс] – Режим доступу: https://www.spiceworks.com/it-security/vulnerability-management/articles/best-threat-intelligence-platforms/

8. Aws Amazom [Електронний ресурс] – Режим доступу: https://aws.amazon.com/ru/

9. BAE systems[Електронний ресурс] – Режим доступу: https://www.baesystems.com/

10. Anti-malware [Електронний ресурс] – Режим доступу: https://www.anti-malware.ru

11. Helpnet security [Електронний ресурс] – Режим доступу: https://www.helpnetsecurity.com/2022/04/04/role-ciso/

12. Symantec-enterprise [Електронний ресурс] – Режим доступу: https://symantec-enterprise-blogs.security.com/blogs/feature-stories/growing-challenges-threat-detection-and-response

13. Av-test [Електронний ресурс] – Режим доступу: https://www.av-test.org/en/statistics/malware/

# ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)