НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

«До захисту допущено»
В.о. завідувача кафедри

_____ М.В.Грайворонський
(підпис)

“_____”_____2019 р.

Дипломна робота

на здобуття ступеня бакалавра

з напряму підготовки 6.170101 «Безпека інформаційних і комунікаційних систем»

на тему: Розробка методики аналізу стану безпеки інформаційної системи за допомогою програми Splunk

Виконав: студент 4 курсу, групи ФБ-52

Олійник Володимир Володимирович_____ _____
(прізвище, ім’я, по батькові) (підпис)

Керівник доцент, кандидат фізико-математичних наук, Орєхов О.А. ___ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Рецензент_____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ - 2019 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – перший (бакалаврський)

Напрям підготовки 6.170101 «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ М.В.Грайворонський
(підпис)

«___»_____2019 р.

ЗАВДАННЯ
на дипломну роботу студенту

Олійник Володимир Володимирович _____
(прізвище, ім'я, по батькові)

1. Тема роботи Розробка методики аналізу стану безпеки інформаційної системи за допомогою програми Splunk,

науковий керівник роботи Орєхов Олександр Арсенійович, кандидат фізико-математичних наук,

затверджені наказом по університету від «____ » 2019 р. № _____

2. Термін подання студентом роботи 10 червня 2019 р.

3. Вихідні дані до роботи _____
_____
_____

4. Зміст роботи_____
_____
_____
_____
_____

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо) _____
_____
_____
_____

6. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка

Студент _____ В.В. Олійник
(підпис) (ініціали, прізвище)

Науковий керівник роботи _____ О.А. Орєхов
(підпис) (ініціали, прізвище)

РЕФЕРАТ

Обсяг пояснювальної записки становить 60 сторінок, у роботі додано 20 ілюстрацій, також робота містить 5 таблиць та 29 джерел за переліком посилань;

Об’єктом дослідження є безпека інформаційних та комунікаційних систем. Предметом дослідження є аналіз безпеки інформаційної системи за допомогою програми Splunk.

Методами дослідження є експериментальний – ми провели експеримент, у якому зробили аналіз стану безпеки операційної системи Metasploitable 2 з відоми станом безпеки. Порівняльний – ми порівняли отримані результати з очікуваними, які були відомі з документації вибраної для аналізу операційної системи. Формалізація – ми формалізували отримані результати у таблиці та діаграми.

В результаті роботи була одержана нова методика аналізу стану безпеки інформаційної системи за допомогою програми Splunk. Показником успішності методики став, експеримент у якому отримані результати, порівняні з очікуваними підтвердили спроможність запропонованої методики аналізу стану безпеки інформаційної системи за допомогою програми Splunk.

Результати роботи може бути використання методики на підприємстві для аналізу стану безпеки інформаційної системи. Розробка лабораторної роботи на основі методики для навчання майбутніх спеціалістів.

Напрямом продовження дослідження розробка інших методик для роботи з SIEM-ситемами та програмою Splunk.

SIEM-ситемами, програма Splunk, аналіз стану безпеки інформаційної системи, журналювання логів, кореляційний пошук, помітні події, ОС Metsploitable 2.

ABSTRACT

The volume of the explanatory note is 57 pages, in the work there are 20 illustrations, also the work contains 5 tables and 29 sources under the list of references;

The object of research is the safety of information and communication systems. The subject of the study is an analysis of the security of the information system with the help of the program Splunk.

The research methods are experimental - we conducted an experiment in which the security status analysis of the operating system Metasploitable 2 was made known to the state of security. Comparative - we compared the results with the expected results that were known from the documentation selected for the analysis of the operating system. Formalization - we formalized the results obtained in the table and diagram.

As a result of the work, a new method for analyzing the security status of the information system with the help of Splunk was obtained. An indicator of the success of the method became, the experiment in which the results obtained, compared with the expected, confirmed the ability of the proposed method for analyzing the state of security of the information system with the help of the program Splunk.

The results of the work may be the use of a methodology at the enterprise to analyze the security status of the information system. Development of laboratory work based on the methodology for training future specialists.

The direction of continuation of research is the development of other methods for working with SIEM systems and the program Splunk.

SIEM sytems, Splunk program, security analysis of the information system, journal logging, correlation search, notable events, OC Metsploitable 2.

ЗМІСТ

Перелік умовних позначень, символів, одиниць, скорочень і термінів….7

Вступ…….8

1 SIEM-системи та програма Splunk. Проблема методології……..10

1.1 SIEM-системи……...……10

1.2 Програма Splunk. Особливості та можливості Splunk…….12

1.3 Проблема методології…….21

Висновки до першого розділу……24

2 Методика аналізу стану безпеки ІС за допомогою програми Splunk…..26

2.1 Логування за допомогою Splunk……26

2.2 Застосування основних елементів Splunk IT Service Intelligence……..31

2.3 Помітні події у Splunk……33

2.4 Боротьба з кіберзлочинністю з аналітикою Splunk Security..…36

Висновки до другого розділу……38

3 Аналіз стану безпеки Metasploitable 2 за методикою аналізу стану безпеки ІС за допомогою програми Splunk……39

3.1 Обґрунтування вибору ІС…….39

3.2 Установка програми Splunk та ОС Metasploitable 2..……41

3.3 Аналіз стану безпеки…….44

3.4 Аналіз результатів……..…50

Висновки до третього розділу……....53

Висновки……..…54

Перелік джерел посилань……...58

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

CaaS - Crime as a Service, злочин як послуга.

HR – Human Resources.

IIoT - Industrial Internet of Things, система для корпоративного або галузевого застосування - відрізняється від звичайного IoT тим, що підключаються промислові (виробничі) об'єкти з вбудованими датчиками.

IoT - Internet of Things, система об'єднаних комп'ютерних мереж і підключених фізичних об'єктів (речей) з вбудованими датчиками і ПО для збору та обміну даними, з можливістю віддаленого контролю і управління в автоматизованому режимі, без участі людини.

ITSI - IT Service Intelligence.

KPI - Key Performance Indicators, Ключові показники ефективності.

SIEM - Security Information and Event Management, програмні продукти, які об'єднують управління інформаційною безпекою та управління подіями безпеки.

SPL - Search Processing Language, спеціальна мова для Splunk.

SQL - Structured Query Language, спеціальна мова для реляційних баз даних.

БД – База Даних.

ІС – Інформаційна система.

ІТ – інформаційні технології.

ОС – операційна система.

ВСТУП

Актуальність роботи:

Проблема якісного аналізу безпеки дуже актуальна у сучасній Україні, оскільки ІС стає все більше. Успішність роботи системи напряму залежить від стану безпеки ІС. У кожній компанії є цілий відділ, який займається цим питанням, а у передових вузах є численні спеціальності, які цьому присвячені.

Splunk одна з передових програм в аналізі безпеки, вона має дуже великий набір можливостей і з успіхом використовується по всьому світу. В Україні їй приділено мало уваги, але вона набирає популярності і в майбутньому може зайняти лідерство.

Через те, що Splunk почали використовувати в Україні відносно нещодавно, існує проблема методології. Матеріалів з використанням Splunk дуже мало, і здебільшого це дуже вузькоспеціалізовані гайди або рішення однієї проблеми або задачі з використання Splunk. В цій роботі ми розглядаємо програму Splunk, як інструмент аналізу стану безпеки ІС, і ми можемо зазначити, що не існує жодної методики з комплексного аналізу стану безпеки ІС. Саме цю проблеми було прийнято рішення вирішити у даній роботі.

Мета і завдання дослідження

Мета роботи удосконалити методи аналізу безпеки ІС, шляхом розробки методики аналізу стану безпеки за допомогою програми Splunk. Перед нами стоять завдання:

1) Дослідити методи аналізу безпеки ІС за допомогою програми Splunk.
2) Розробити методику аналізу безпеки ІС за допомогою програми Splunk.

3) Зробити аналіз стану безпеки Metasploitable 2 за допомогою програми Splunk, для підтвердження успішності запропонованої методики.

Об’єктом дослідження є безпека інформаційних та комунікаційних систем.

Предметом дослідження є Аналіз безпеки ІС за допомогою програми Splunk.

Методи дослідження

Експериментальний – ми провели експеримент, у якому зробили аналіз стану безпеки ОС Metasploitable 2. Порівняльний – ми порівняли отримані результати з очікуваними, які були відомі з документації вибраної для аналізу ОС. Формалізація – ми формалізували отримані результати у таблиці та діаграми.

Наукова новизна одержаних результатів

В результаті роботи була одержана нова методика аналізу стану безпеки ІС за допомогою програми Splunk. Показником успішності методики став, експеримент у якому отримані результати, порівняні з очікуваними підтвердили це.

Практичне значення одержаних результатів

Використання методики на підприємстві для аналізу стану безпеки інформаційної системи

Розробка лабораторної роботи на основі методики для навчання майбутніх спеціалістів.

1 SIEM-СИСТЕМИ ТА ПРОГРАМА SPLUNK. ПРОБЛЕМА МЕТОДОЛОГІЇ.

1.1 SIEM-системи

SIEM у комп'ютерній безпеці є програмними продуктами, які об'єднують управління інформаційною безпекою та управління подіями безпеки. Технологія SIEM забезпечує аналіз в реальному часі подій безпеки, отриманих від мережевих пристроїв і додатків. SIEM представлено додатками, приладами або послугами, і використовується також для журналювання даних і генерації звітів в цілях сумісності з іншими бізнес-даними. Постачальники продають SIEM як програмне забезпечення, як прилади або як керовані послуги; ці продукти також використовуються для реєстрації даних безпеки та створення звітів для цілей відповідності [1].

SIEM-системи здійснюють моніторинг ІС, аналізують події безпеки у реальному часі, які надходять від мережевих пристроїв, засобів захисту інформації та допомагають виявити інциденти інформаційної безпеки. SIEM-системи слугують для моніторингу та реагування на інциденти, але не захищають від ймовірних загроз або від негативних подій. Тобто SIEM слугують для консолідації даних, збір подій інформаційної безпеки з різних джерел; зберігання подій інформаційної безпеки в історичному порядку для ретроспективного аналізу та визначення послідовності дій, які стали причинами появи інцидентів безпеки; кореляція та обробка подій безпеки, використання різних технічних засобів для аналізу даних аудиту; надання інструментів для експертного аналізу подій та інцидентів для побудови зв’язку подій між собою.

SIEM-системи використовують велику кількість джерел даних, щоб надати максимально повне охоплення подій, які регіструються в ІС. SIEM-

системи використовують інформацію з таких джерел: системи автентифікації та системи контролю та керування доступом; антивірусні засоби; між мережеві екрани; системи виявлення та запобігання вторгнень; системи проксіювання доступу в інтернет та веб-фільтрації; активні мережеві пристрої; системні журнали подій інформаційної безпеки серверів та робочих станцій користувачів; журнали аудита систем керування базами даних. Отриману інформацію SIEM-системи аналізують за допомогою правил, які включають набір вимог, тригерів, лічильників і сценаріїв відповідних дій. SIEM-системи не протидіє злим намірам дій порушників, але дозволяє отримати найбільш повне уявлення про події безпеки, що виникають.

SIEM — це складна комплексна система, яка дозволяю отримати своєчасну та повну інформацію по стан ІС. SIEM-системи є дуже непростими та дорогими інструментами керування електронними журналами. Складний процес впровадження та вимоги до безперервного забезпечення збору подій та керування правилами кореляції вимагає наявності в штаті кваліфікованих співробітників.

У разі успішного впровадження та експлуатації SIEM-системи буде здійснена кореляція та обробка подій безпеки. Також дає можливість побудови систем та центрів моніторингу та реагування, автоматизацію процесів виявлення загроз та аномалій, автоматизацію процесів реєстрації та контролю інцидентів, з подальшою можливістю їх розслідування. Дозволяє реагувати на загрози, що виникають, в режимі реального часу [2].

В Україні в сьогоднішніх економічних та політичних умовах ринок SIEM розвивається повільніше, ніж за кордоном. Не всі світові лідери мають представництва в нашій країні. Хоча спостерігається позитивна тенденція в розвитку.

1.2 Програма Splunk. Особливості та можливості Splunk

1.2.1 Програма Splunk

Splunk - американська компанія, розробник програмного забезпечення для обробки та аналізу машинно-генеруються даних. Штаб-квартира знаходиться в Сан-Франциско. Компанія заснована в 2003 році Майклом Баумом, Еріком Своном і Робом Дасом. Основний однойменний продукт випущений вперше 2006 році. У 2011 році був випущений продукт Splunk Storm - хмарна версія основної системи Splunk. У 2013 році компанія випустила новий продукт Hunk, призначений для обробки і аналізу великих обсягів даних, що зберігаються в Hadoop.

Основний програмний продукт - однойменна система аналізу операційної діяльності в області інформаційних технологій, що збирає і аналізує великі обсяги машинних даних з усіх фізичних, віртуальних і хмарних середовищ IT-інфраструктури організації. Зібрані дані індексуються, в час доступу до даних, записаним раніше без моделювання, система перетворює машинні дані в формат «ключ - значення», після цього дані стають доступними для пошуку та аналізу через веб-інтерфейс. У продукті не використовується будь-яка зумовлена схема обробки даних, і орієнтована на роботу довільними форматами з системних журналів.

Система дозволяє здійснювати пошук як за даними в реальному часі, так і за архівними даними, на основі результатів пошуку Splunk дає можливість: аналізувати отримані результати за допомогою засобів візуалізації, формувати звіти і попередження, створювати систему моніторингу та повідомлень в реальному часі. Передбачена можливість розширення - можна створювати нові додатки засобами спеціалізованої платформи розробки, що поставляється зі Splunk.

Застосовується для пошуку і усунення неполадок в IT-інфраструктурі, моніторингу порушень системи безпеки, запобігання атак, отримання інформації для бізнес-аналітики, оптимізації робочого процесу підприємства і збільшення продуктивності, для роботи з різноманітними великими масивами промислових даних[3].

Продукт має два типи ліцензій - безкоштовну і корпоративну. Ліцензування здійснюється на основі щодня оброблюваного обсягу даних. Безкоштовна версія Splunk дозволяє індексувати до 500 Мбайт даних в день. У корпоративної версії немає обмежень за обсягом даних; в порівнянні з безкоштовною версією вона підтримує розгортання в багатокористувацького, розподіленого середовища і включає в себе функцію генерації попереджень, рольову модель безпеки, технологію єдиного входу, доставку файлу PDF за розкладом та інші можливості[4].

1.2.2 Аналітика роботи додатків

В даний час бізнес спирається на додатки для обробки практично кожного процесу. Низький рівень задоволеності якістю роботи цих додатків може поставити під загрозу репутацію, конкурентні переваги і в кінцевому підсумку дохід. Тому отримання інсайдів з додатків та інфраструктури, на якій вони працюють, стає важливим завданням для будь-якого бізнесу.

Splunk дозволяє агрегувати машинні дані про використання додатків, їх доступності та продуктивності. Дані можуть збиратися з широкого спектру джерел в режимі реального часу.

Splunk дозволяє вимірювати в режимі реального часу доступності додатків, продуктивності і використання користувачами сприяє можливості забезпечення високої якості обслуговування і отримання позитивного клієнтського досвіду. Коли ви комбінуєте видимість машинних даних на

різних рівнів вашої інфраструктури з моніторингом в реальному часі, ви може передбачати події навіть до того, як вони відбулися.

Ми можемо скоротити середній час на відновлення працездатності системи і на усунення неполадок, визначаючи причини збоїв в роботі і вузькі місця системи. Розподілені додатки можуть генерувати багато помилок, а корінь проблеми знайти не просто, так як розробники додатків і адміністратори можуть не мати прямого доступу до машинних даних, які їм потрібні. Splunk може надати доступ до всіх ваших даних, що дозволить швидко виправити проблеми і скоротити час простою.

За допомогою Splunk можна оптимізувати продуктивність програми та вартість обслуговування за рахунок розуміння використання програми. А також зробити прогноз майбутніх значень і планування потужності, за рахунок машинного навчання.

Частиною можливостей Splunk є аналіз і складання звітності про загальну доступності сервісу і ключових показниках ефективності, а також здатність швидко визначити причину, в разі відхилення від оптимальних значень.

Існує можливість інтегрувати в Splunk не тільки IT-дані, але і дані з джерел не відносяться до IT, дозволяє розробникам і різним бізнес напрямками оцінювати вплив транзакцій на бізнес і то, як додатки сприяють веденню бізнесу.

Для IT-фахівців, які використовують DevOps, програмне забезпечення Splunk допомагає підвищити швидкість і якість роботи над додатками. На відміну від інших рішень, орієнтованих на окремі компоненти розробки, Splunk надає інформацію в реальному часі на всіх етапах життєвого циклу розробки продукту, що дозволяє скоротити час розробки і виходу продукту на ринок[5].

Таким чином, аналітика роботи додатків в Splunk дозволяє:

- Поліпшити продуктивність додатків, шляхом виявлення проблем, які зачіпають доступність і швидкодія

- Скоротити середній час на відновлення працездатності системи і усунення неполадок
- Отримати інформацію використання додатків, включаючи поведінку користувачів і продуктивність програми
- Поліпшити DevOps і зменшити час виходу на ринок продукту

1.2.3 Аналітика подій безпеки

У реаліях сьогоднішнього дня підприємствам уже недостатньо простого моніторингу традиційних подій, їм потрібні рішення, здатні адаптуватися до сучасних загроз, що прискорюють швидкість реагування на інциденти і дають можливість виявляти і усувати відомі і невідомі загрози.

Прискорення реакції є складним завданням в сучасних складних IT-середовищах. Splunk створює чіткі наочне уявлення про стан безпеки організації в поточний момент, а також містить зручну настройку уявлень і деталізацію даних аж до базових подій. Використання безперервного моніторингу, статичних і динамічних пошуків або візуальних кореляцій для визначення шкідливої активності скорочує час реагування. А також Splunk надає аналітикам інструменти для визначення пріоритетів для більш швидкого реагування на загрози з більш високим пріоритетом.

За допомогою Splunk можна відстежувати різні стадії складної загрози і об'єднувати взаємопов'язані події. Взаємозв'язку визначаються по будь-якому полю, будь-яких даних і на будь-якому часовому інтервалі. Splunk дозволяє аналітикам безпеки застосовувати розширений статистичний аналіз і методи машинного навчання для виявлення викидів і аномалій, які дозволяють виявити невідомі і складні загрози.

Splunk служить для виявлення зловмисних дій співробітників та інших внутрішніх загроз до того, як станеться крадіжка конфіденційних даних, їх пошкодження або зловживання повноваженнями. За допомогою Splunk можна визначити неправильне використання дозволів, аномальна поведінка, навіть в разі використання законних облікових записів, рівнів доступу або джерел. Наприклад, надмірно тривалі сеанси, нестандартне час або входу. А що накопичуються дані про різні дії користувача дозволяють засновувати дослідження на історичних даних. У Splunk можлива інтеграція з Active Directory або базами даних HR для отримання інформації про співробітників.

Splunk дозволяє аналізувати інциденти для визначення обставин і масштабів інциденту. Це досягається за допомогою пошуку і знаходження кореляцій за ключовими словами, термінам або значенням для різних мережевих пристроїв, хостів, зчитувачів тощо. Для аналітиків безпеки це дає широкий контекст інциденту, що допомагає швидше і краще оцінювати рівень загрози, визначати причини і наслідки.

Архітектури безпеки зазвичай включають в себе різні рівні інструментів і продуктів. Як правило, вони не призначені для спільної роботи і містять прогалини в питаннях роботи фахівців з безпеки по установці зв'язків між різними доменами. Splunk усуває ці прогалини, забезпечуючи єдиний інтерфейс для автоматичного отримання даних, що дозволяє будувати комплексну аналітику і реагувати на загрози в середовищах з продуктами різних постачальників.

За допомогою пошуку та аналізу даних в реальному часі, виявлення і дослідження викидів і аномалій на основі історичних даних можна виявити шахрайські дії, визначити вплив і масштаб шахрайства[6].

1.2.4 Splunk для IoT

Інтернет Речей (IoT) - система об'єднаних комп'ютерних мереж і підключених фізичних об'єктів (речей) з вбудованими датчиками і ПО для збору та обміну даними, з можливістю віддаленого контролю і управління в автоматизованому режимі, без участі людини.

Промисловий Інтернет Речей (IIoT) - інтернет речей для корпоративного або галузевого застосування - відрізняється від звичайного IoT тим, що підключаються промислові (виробничі) об'єкти з вбудованими датчиками.

Всі ці об'єкти генерують величезну кількість структурованих і неструктурованих даних. При обробці цих даних можна отримати інформацію, яка може бути використана для запобігання поломок обладнання, позапланових простоїв, скорочення позапланового техобслуговування і збоїв в управлінні ланцюгами поставок, тим самим дозволяючи підприємству функціонувати більш ефективно.

Зараз у всьому світі промислове виробництво все частіше звертається до своїх даних IIoT, щоб краще контролювати і діагностувати проблеми роботи обладнання, а також прогнозувати потреби в обслуговуванні.

За дослідженнями ARC Industry, глобальна обробна промисловість щорічно втрачає 20 мільярдів доларів з незапланованих простоїв, і майже 80% промислових операцій є реактивними[7]. Відсутність усвідомлення в режимі реального часу того, що відбувається в критичних промислових системах, викликає реактивний підхід до управління промисловими операціями, а виникаючі проблеми часто вирішуються за допомогою інтуїції, а не з використанням підходу, заснованого на даних.

У цій ситуації особливого значення набуває коректне уявлення актуальною та своєчасною інформацією в зрозумілому для користувача вигляді.

Програмне забезпечення Splunk дозволяє збирати, аналізувати і візуалізувати дані в режимі реального часу, а також зіставляти історичні дані з будь-якого джерела, включаючи дані, які генеруються різними датчиками, сенсорами, мережами і додатками, пов'язаними з промисловим виробництвом[8].

Основні можливості Splunk для роботи з промисловими даними:

1) Моніторинг та діагностика:

- Постійний моніторинг і збір даних в режимі реального часу
- Комбінування і зіставлення даних різних джерел: датчиків, інфраструктури, додатків
- Отримання і обробка не тільки неструктурованих даних, але і інтеграція з класичними базами даних
- Можливість в одному місці отримувати показники, пов'язані з продуктивністю промислового обладнання, і бізнес показники. Це дає широкий контекст для прийняття рішень з різних проблем

2) Безпека і відповідність вимогами:

- Швидке усвідомлення ризику за рахунок всебічної прозорості в режимі реального часу для відстеження продуктивності важливих активів
- Проведення швидких розслідувань за допомогою спеціальних пошуків і динамічних візуальних кореляцій, які ідентифікують аномальні дії
- Скорочення часу простою виробництва за рахунок зменшення кількості збоїв в системі

3) Предиктивне обслуговування

- Прогноз часу простою критично важливих виробничих об'єктів за допомогою машинного навчання

- Моніторинг працездатності обладнання і скорочення перевантажень за допомогою аналізу досягнення порогових значень, аварійних сигналів, індикаторів і різних тенденцій[8].

На даний момент, існує більше 100 додатків і надбудов IoT для завантаження даних з різних сенсорів, датчиків і обладнання в Splunk.

Навесні 2018 року Splunk оголосила про запуск своєї першої платформи Splunk Industrial Asset Intelligence, безпосередньо пов'язаної з IIoT, призначеної для інженерів з автоматизації процесів в промислових компаніях. Це рішення призначене для компаній в сфері виробництва, енергетики, транспорту, нафти і газу, а також інших промислових галузей[4].

1.2.5 Основні відмінності та сильні сторони Splunk

Splunk, в більшості випадків, розбирає вхідні дані на поля і значення і надалі обробляє їх. Обробка відбувається за допомогою SPL запитів, за допомогою якого можна будувати різні вибірки і таблиці, сортувати, фільтрувати, агрегувати, будувати звіти, створювати обчислювані поля, звертатися як до внутрішніх, так і зовнішніх довідників і робити алерт

Splunk здійснює збір, пошук, моніторинг та аналіз за різними і досить великим (сотні терабайт даних в день) обсягами даних в режимі реального часу і все це одна система.

Splunk може забезпечити збір даних в реальному часі з тисяч різнорідних джерел - і це може бути як фізичний або віртуальний хост, так і хмара. Також Splunk підтримує пошук не тільки в реальному часі, а й по всьому тимчасовому проміжку, дані за який були зібрані. Тобто ми можемо здійснювати пошук, моніторинг, оповіщення, звітність і аналіз за будь-який

час. І нарешті, Splunk забезпечує швидкий результат і високу інтерактивність пошукових запитів на надзвичайно великих обсягах даних.

Splunk є універсальною платформою для машинних даних, яка забезпечує комплексний збір даних, їх обробку та аналіз. Таким чином ми можемо індексувати будь-які машинні дані з відміткою про час незалежно від структури і формату. Splunk здатний об'єднати в собі машинні дані + бізнес дані + призначені для користувача дані, що робить його вкрай універсальним.

Splunk здійснює пошуки за часом, тобто вам не потрібно заздалегідь знати структуру даних, щоб сформувати запит. Ви можете вибрати проміжок в часі, ввести пару ключових слів і швидко ознайомитися з даними. Немає ніяких жорстких обмежень на стовпці, таблиці та інше. Це сильно підвищує гнучкість системи. Також будь-який запит можна зупинити, поставити на паузу або показати проміжні результати.

Splunk надає широкі можливості з побудови аналітики, звітів та їх візуалізації. Крім цільових даних, система також може звертатися до зовнішніх довідників, наприклад в SQL БД. Також хотілося б сказати, що Splunk досить відкрита система і ви завжди можете дописати свій модуль.

Splunk використовує технологію MapReduce, що забезпечує розподіл навантажень і горизонтальну масштабованість системи, тобто ми можемо почати з одного сервера для Splunk, а при збільшенні даних - швидко додати пару нових серверів і розподілити навантаження. Також завдяки технології MapReduce Splunk може швидко переробляти реально великі обсяги даних.

Splunk дозволяє швидко отримати результат від використання. Впровадження займає години або дні, а не тижні і місяці. Теж саме з масштабуванням і експлуатацією[9].

У Splunk є дуже якісне, а головне безкоштовне ком'юніті, яке включає:

- Splunk Base - портал, що містить всілякі додатки, більшість з яких безкоштовні.
- Splunk Answers - форум з великим числом питань та відповідей і живих учасників.
- Splunk Dev - портал для розробників.
- Splunk Dock - повна база знань продукту.

1.3 Проблема методології

1.3.1 Splunk на ринку України

Виходячи з вищесказаного, а так же, через простоту використання та дедалі більшої актуальності, продукти Splunk б'ють всі рекорди з продажу на світових ринках[2]. Завдяки цьому, Splunk отримав багато нагород, та входить до численних рейтингів: Splunk увійшов до списку CRN 2019 Big Data 100 в категорії «Управління великими даними і інтеграція»[10], Splunk увійшов до списку кращих компаній LinkedIn 2019 року[11], Splunk був названий переможцем в списку G9 Crowd's 2019 Best Software Products Awards, зайнявши 4-е місце в загальному заліку[12]. Без сумніву, рішення Splunk стають досить затребуваними і для України.

В 2016 компанія «RRC Україна» приносить в Україну інноваційний продукт - програмне забезпечення для обробки та аналізу машинно-генеруються даних від компанії Splunk. Фахівці компанії вперше на території України провели навчання SplunkGettingStarted.

На заході проведеному «RRC Україна» були присутні понад 30 слухачів, що представляє справжній зріз великого українського бізнесу,

всіх форм власності. Інтерес до американського вендору Splunk і його додатком був досить значним і після заходу, про що свідчать письмові звернення від слухачів, які прийшли вже після навчання.

На той момент компанія «RRC Україна» була ексклюзивним дистриб'ютором продукції Splunk на території України. Компанія була готова посприяти в розгортанні пілотних проектів, які допоможуть визначитися з необхідністю подальшого впровадження Splunk[13].

Але у 2018, а можливо і раніше, в Україні вже проводяться тендери на закупівлю програмного забезпечення Splunk[14]. На ринку з’являється конкуренція, це свідчить про його розвиток, а також про привабливість для компаній. Отже Splunk має великий попит, і може у майбутньому стати лідером своєї галузі.

Слід зазначити, що відставання в Україні від темпів інтеграції Splunk за кордоном здебільшого пов’язано не з використанням самої програми Splunk, а SIEM-систем в цілому. Але зараз українські IT компанії зрозуміли, що безпека ІС повинна була в пріоритеті, адже це безпосередньо впливає на прибутки. Поліпшення якості обслуговування клієнтів, скорочення величини втраченого прибутку за рахунок скорочення збоїв у роботі, скорочення часу виявлення причини інциденту від годин до декількох хвилин або секунд, прискорення часу виходу на ринок, надаючи розробникам продуктів дані роботи додатків в режимі реального часу це все дозволяє використання SIEM-систем та зокрема інтеграція Splunk.

1.3.2 Проблема методології

Через те, що Splunk почали використовувати в Україні відносно нещодавно, існує проблема методології. Матеріалів з використанням Splunk дуже мало, і здебільшого це дуже вузькоспеціалізовані гайди або рішення

однієї проблеми або задачі з використання Splunk. В цій роботі ми розглядаємо програму Splunk, як інструмент аналізу стану безпеки ІС, і ми можемо зазначити, що не існує жодної методики з комплексного аналізу стану безпеки ІС. Саме цю проблеми було прийнято рішення вирішити у даній роботі.

Трішки краще ситуація з матеріалами на англійській мові. Нам вдалося знайти дві книги, які присвячені Splunk, але в них розповідається про саму програму Splunk та її можливості. Це Splunk Operational Intelligence Cookbook[15] та Implementing Splunk Big Data Reporting and Development for Operational Intelligence[16]. У книгах розглядаються багато тем, з якими ви зіткнетеся при роботі зі Splunk, починаючи з завантаження даних, закінчуючи створенням аналітичних звітів з використанням мов XML і Python. В другій робиться акцент на «advanced» методиках пошуку, візуалізації, архітектури Splunk тощо. Але не можна сприймати ці книги як методики з аналізу стану безпеки ІС. Також слід зазначити, що книги не можливо обновити, разом з обновленням програми, тому деякі приклади та використані функції, можуть вже бути зміненими у нових версіях програми.

Існує офіційний керівництво - основне джерело, з якого можна отримати всю актуальну інформацію про роботу в Splunk. Все, що можна реалізувати в Splunk, ви можете знайти тут: інструкцію щодо завантаження різних типів даних з різних джерел, докладну довідку по кожній функції мови SPL, інструкцію по всім способам візуалізації і створення звітності, керівництво по адмініструванню системи, усунення неполадок тощо. Кожна сторінка має кілька версій в залежності від того, інформація про яку версію Splunk вам потрібна. Серед мінусів цього керівництва хочеться відзначити, що там занадто багато інформації, щоб легко знайти саме те, що потрібно. А також складна система гіперпосилань з однієї теми на іншу. Часто доводиться прочитати розділ повністю. Але це не методика для вирішення

конкретної проблеми або задачі, а тим це не методика для аналізу безпеки ІС, яка нас цікавить[17].

Якщо говорити про російську мову, яку знає більшість українців є збірка посилань від TS Solution на усі ресурси з інформацією про програму Splunk[18]. Але це лиже посилання, це не може бути методикою.

Отже ми маємо достатньо інформації про програму Splunk, але немає комплексних методик для вирішення загальних проблем. Наприклад, методики аналізу стану безпеки ІС.

Висновки до першого розділу

В розділі було розглянуто роль SIEM-систем у захисті ІС. У разі успішного впровадження та експлуатації SIEM-системи буде здійснена кореляція та обробка подій безпеки. Також дає можливість побудови систем та центрів моніторингу та реагування, автоматизацію процесів виявлення загроз та аномалій, автоматизацію процесів реєстрації та контролю інцидентів, з подальшою можливістю їх розслідування. Дозволяє реагувати на загрози, що виникають, в режимі реального часу [2].

В Україні в сьогоднішніх економічних та політичних умовах ринок SIEM розвивається повільніше, ніж за кордоном. Не всі світові лідери мають представництва в нашій країні. Хоча спостерігається позитивна тенденція в розвитку.

Було детально розглянуто програму Splunk. Вона дозволяє швидко отримати результат від використання. Впровадження займає години або дні, а не тижні і місяці. Теж саме з масштабуванням і експлуатацією[9]. Splunk є універсальною платформою для машинних даних, яка забезпечує комплексний збір даних, їх обробку та аналіз. Splunk дозволяє аналізувати

інциденти для визначення обставин і масштабів інциденту. Система дозволяє здійснювати пошук як за даними в реальному часі, так і за архівними даними, на основі результатів пошуку Splunk дає можливість: аналізувати отримані результати за допомогою засобів візуалізації, формувати звіти і попередження, створювати систему моніторингу та повідомлень в реальному часі[3]. За допомогою Splunk можна оптимізувати продуктивність програми та вартість обслуговування за рахунок розуміння використання програми. А також зробити прогноз майбутніх значень і планування потужності, за рахунок машинного навчання[5].

Без сумніву, рішення Splunk стають досить затребуваними і для України. Зараз українські IT компанії впевнені, що безпека ІС повинна бути в пріоритеті, адже це безпосередньо впливає на прибутки. Поліпшення якості обслуговування клієнтів, скорочення величини втраченого прибутку за рахунок скорочення збоїв у роботі, скорочення часу виявлення причини інциденту від годин до декількох хвилин або секунд, прискорення часу виходу на ринок, надаючи розробникам продуктів дані роботи додатків в режимі реального часу це все дозволяє використання SIEM-систем та зокрема інтеграція Splunk.

Наприкінці була піднята проблему методології SIEM-систем та зокрема програми Splunk. Ми маємо достатньо інформації про програму Splunk, але немає комплексних методик для вирішення загальних проблем. Наприклад, методики аналізу стану безпеки ІС.

2 МЕТОДИКА АНАЛІЗУ БЕЗПЕКИ ІС ЗА ДОПОМОГОЮ ПРОГРАМИ SPLUNK.

2.1 Логування за допомогою Splunk

У цьому пункті методики представлені дії, які необхідні для моніторингу логів систем безпеки і для оперативного реагування на інциденти безпеки, а також перелік можливих джерел і подій, які можуть представляти інтерес для аналізу.

Крок перший. Визначити, які джерела журналів і автоматизовані інструменти можна використовувати для аналізу.

Потенційні джерела логів безпеки(див.рис.2.1):

- Журнали операційної системи серверів і робочих станцій
- Журнали додатків (наприклад, веб-сервер, сервер баз даних)
- Журнали інструментів безпеки (наприклад, антивірус, інструменти виявлення змін, системи виявлення або запобігання вторгнень)
- Вихідні журнали проксі-сервера і журнали додатків кінцевих користувачів

- інші джерела подій безпеки, що не входять в журнали.

Стандартне розташування логів:

- Операційна система Linux: / var / log
- Операційна система Windows: Windows Event Log (Security, System, Application)
- Мережеві пристрої: зазвичай реєструються через syslog; деякі використовують власне розташування і формати

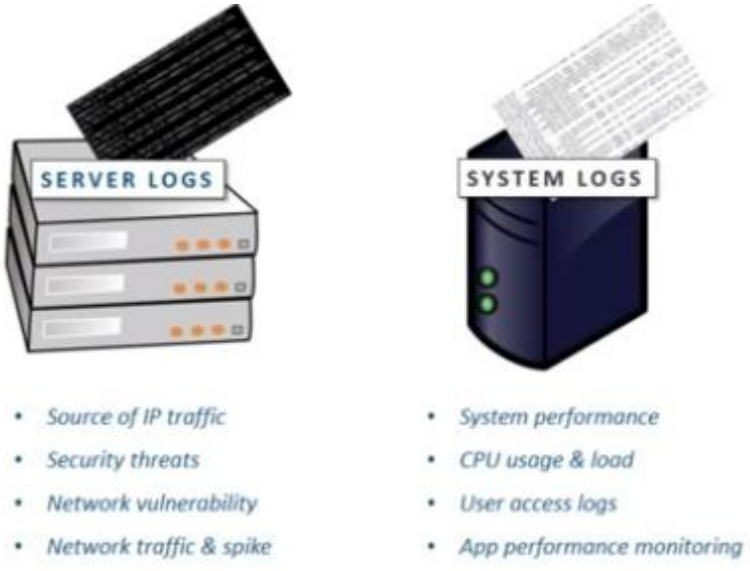

Рисунок 2.1 – Джерела логів

Крок другий. Скопіювати записи журналу в одне місце, де ми зможемо всі їх переглянути і обробити. Цей крок не актуальний для Splunk, тому що програма має доступ до всіх логів в ІС і ми можемо за допомогою пошуку знайти ті логи, які нас цікавлять.

Крок третій. Створити правила визначення того, що події є необхідними нам, щоб в автоматичному режимі зменшувати накопичення логів.

Рисунок 2.2 - Логи

Пошук у логах повинен складатися зі спеціальних вузьконапрямлених запитах. Для цього існують ключові слова у логах, які відносяться до певної події. (див. табл. 2.1)

Таблиця 2.1 – Пошук у логах, ключові слова. Система Linux

Подія	**Приклад запису у логах**
Успішний вхід	«Accepted password», «Accepted publickey», «session opened»
Невдалі спроби входу	«authentication failure», «failed password»
Завершення сесії	«session closed»
Зміна аккаунту	«password changed», «new user», «delete user»
Дії від Sudo	«sudo:…COMMAND=...», «FAILED su»
Збої в роботі	«failed» або «failure»

У системі Windows замість ключових слів є id події, саме за ним ми будемо робити пошук у логах. (див. табл. 2.2)

Таблиця 2.2 – Пошук у логах, id події. Система Windows

Подія	**EventID**
Події входу і виходу	Successful logon 4624; failed logon 4625; logoff 4634, 4647
Зміна аккаунту	Created 4720; enabled 4726
Зміна пароля	Changed 4738; disabled 4725; deleted 630
Запуск і припинення роботи сервісів	4724, 4723
Доступ до об'єктів	7035,7036

Окрім самої система, треба виконати пошук у логах мережевих пристроїв. (див. табл. 2.3)

Таблиця 2.3 – Пошук у логах, ключові слова. Мережеві пристрої

Подія	**EventID**
Трафік, допущений файерволом	«Built ... connection» «access-list ... permitted»
Трафік, заблокований файерволом	«access-list ... denied», «deny Inbound»; «Deny ... by»
Обсяг трафіку (в байтах)	«Teardown TCP connection ... duration ... bytes ...»
Використання каналів і протоколів	«limit ... exceeded», «CPU utilization»
Виявлення атаки	«attack from»
Зміна аккаунта	«user added», «user deleted», «User priv level changed»
Доступ адміністратора	«AAA user ...», «User ... locked out», «login failed»

Та наприкінці зробити пошук у логах веб-серверу:

- Надмірні спроби доступу до неіснуючих файлів
- Код (SQL, HTML), як частина URL-адреси
- Доступ до розширень, які ви не встановлювали

- Повідомлення про зупинку або запуск веб-служби
- Доступ до «ризикованих» сторінок, які приймають для користувача введення даних
- Код помилки 200 (успішний запит) на файлах, які не належать вам
- Помилка аутентифікації: Код помилки 401,403
- Невірний запит: Код помилки 400
- Внутрішня помилка сервера: Код помилки 500[19]

Крок четвертий. Визначити, чи можна покладатися на мітки часу журналів.

Крок п’ятий. Звернути увагу на останні зміни, збої, помилки, зміни стану, доступ і інші події, незвичайні для нашої ІС.

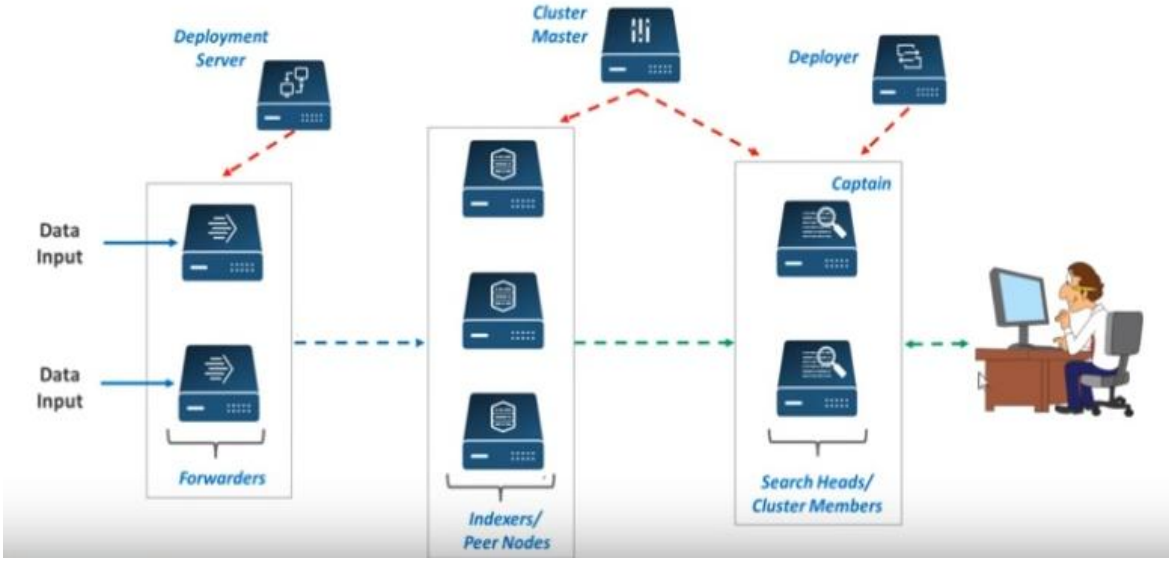

Рисунок 2.3 - Компоненти

Особливістю splunk є те, що в ньому є режим Real-time (див.рис.2.4), в якому нам немає необхідності натискати Search щоб оновити сторінку. Вона оновлюється автоматично при надходженні нових алертів. Виберемо режим Real-time, 1 minute window[29].

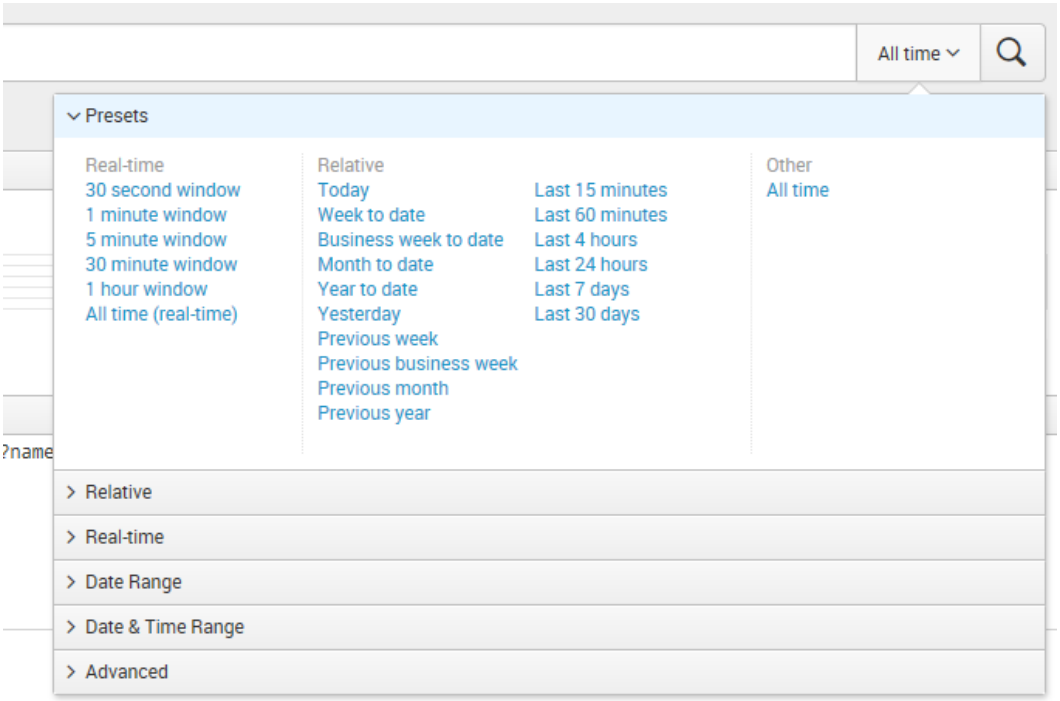

Рисунок 2.4 - Real-time

Крок шостий. Вивчити історію подій, щоб відновити дії до та після інциденту.

Крок сьомий. Зіставити дії в різних журналах, щоб отримати повну картину

Крок восьмий. Сформулювати гіпотезу про те, що сталося; вивчити журнали, щоб підтвердити або спростувати її

2.2 Застосування основних елементів Splunk IT Service Intelligence

Крок перший Service Analyzer.

Отримати найбільш важливу інформацію максимально зрозуміло і швидко, саме для цього служить стартова сторінка ITSI - Service Analyzer. Заходячи в додаток, можна одним поглядом оцінити загальну рівень роботи всієї ІС.

Існує два подання Service Analyzer: вид плитки і деревоподібна структура, яка дозволяє бачити, як одні сервіси впливають на інші.

У вигляді плиток представлені показники працездатності і основні пов'язаними з ними KPI, що мають колірний індикатор і відсортовані за поточним рівнем стану.

Деревоподібне уявлення відображає всі сервіси у вигляді графа, в якому вузли показують рівень працездатності вузла. Кожен вузол можна розкрити і побачити пов'язані з ним показники ефективності.

Крок другий Glass Tables.

Glass Tables є наочною і зручну візуалізацію, яка буде зрозуміла практично будь-якому користувачеві. Таблиці дозволяють дізнатися про стан сервісів і значеннях показників ефективності в інтерфейсі схем роботи або бізнес-процесів. Для зручності можна використовувати різні віджети і значки для відображення показників ефективності KPI.

Крок третій Deep Dives.

Звичайно, бачити тільки стан системи в даний момент, недостатньо. Тому дуже корисно мати можливість моніторингу станів протягом часу. Ми можемо дізнатися як довго триває зниження ефективності роботи чи були проблеми годину-дві або день назад і чому.

У розділі Deep Dives додається історія показників KPI, тобто ми можемо побачити стан системи не тільки зараз, а й кілька годин тому і порівняти результати роботи різних елементів системи в один і той же момент часу або порівняти результати одного сервісу з тим що було день, тиждень або місяць тому.

Крок четвертий Multi KPI Alerts

Часто про проблему нам може сказати тільки сукупність факторів, тому необхідна можливість спрацьовування попереджень, заснованих на декількох KPI або залежних від тривалості досягнення показником якогось певного значення.

У розділі Multi KPI Alerts можливе створення таких композиційних показників ефективності, в яких можна враховувати вагу впливу кожного фактору на загальну проблему[20].

Отже, Services і KPIs показують, які сервіси в даний момент працюють нормально, а які мають відхилення. Glass Tables дозволяють згрупувати показники за специфічними групами і наочно візуалізувати їх. Deep Dives дозволяє порівнювати стан показників в часі і визначати з якого джерела почалася та чи інша проблема. Multu-KPI Alerts виявляють якісь конкретні важливі події і дозволяють керувати ними.

Описані вище додатки не охоплюють на 100% весь функціонал системи, але в цілому дозволяють вирішити основні завданнями компаніям з широкими IT ландшафтами.

2.3 Помітні події у Splunk

2.3.1 Notable Events Review

Крок перший зробити попередній аналіз за допомогою Notable Events Review.

Панель моніторингу «помітних подій» використовується, щоб побачити попередження про проблеми, які в даний час впливають на служби або можуть потенційно вплинути на сервіси. Панель відображає помітні події попередження, що генеруються Multi KPI Alerts, кореляційними пошуками і алгоритмами виявлення аномалій.

Під «помітною подією» може матися на увазі:

- Один з KPI, якщо він перевищує заданий поріг;
- Результат роботи Multi KPI Alerts, який генерує попередження, засноване на стані кількох KPI;

- Результат кореляційного пошуку, який шукає відносини між точками даних.

Для зручності представлення всі події згруповані за допомогою алгоритмів машинного навчання, що визначає схожі події. На інформаційній панелі відображаються відомості про кожну групу подій, такі як кількість подій в групі, часовий діапазон подій в групі, власник, ступінь серйозності, статус і опис. Натиснувши на групу, можна отримати детальну інформацію про події всередині групи.

Ми можемо керувати подіями, встановлювати певні дії і скрипти на реалізацію події, наприклад, відправляти повідомлення на електронну пошту або в зовнішні системи[20].

2.3.2 Кореляційний пошук

Крок другий налаштування кореляційного пошуку.

Splunk описують його як: Подія, що генерується пошуком кореляції як сповіщення. Примітна подія включає в себе спеціальні поля для надання допомоги в розслідуванні умов тривоги та відстеження виправлення подій[22].

Пошук кореляції спеціальний тип запланованого звіту, який дозволяє виявляти підозрілі події та шаблони у ваших даних. Можна налаштувати кореляційний пошук, щоб генерувати помітну подію, коли результати пошуку відповідають конкретним умовам. Ви можете дослідити помітні події, використовуючи інформаційну панель "Огляд подій" у Splunk Enterprise Security[23].

Пошук кореляції працює як будь-який звичайний пошук у Splunk. Безпека підприємства поставляється з рядом важливих подій. Ви можете створювати нові в програмі Enterprise Security App, перейшовши за

посиланням: Налаштувати> Керування вмістом> Створити новий вміст> Пошук кореляції.

Ви можете використовувати будь-який пошук з програми Anomali ThreatStream або створювати власні дані, використовуючи дані збігу індикаторів, отримані за допомогою програми. Ось приклад, який ми скопіюємо один з пошуків з програми ThreatStream App, який сповіщає на основі індикаторів високого пріоритету для APT, C2 або показників шкідливого програмного забезпечення з високою впевненістю, і перетворює його на пошук кореляції[21].

Запит пошуку виглядає так:

| `ts_tstats_all` | `ts_lookup_details` | `ts_get_time_offset(_time, ts_date_last)` | where ts_confidence >= 80 AND Age < 31 AND (like(ts_itype, “apt%”) OR like(ts_itype, “c2%”) OR like(ts_itype, “mal%”)) | eval orig_sourcetype=sourcetype

За потребою можна змінити наведені нижче налаштування, хоча для налаштування пошуку кореляції можна скористатися типовими значеннями за умовчанням[24].

2.3.3 Додавання помітної події та фільтрація помітних подій

Крок третій додати помітну подію та налаштувати фільтрацію.

Якщо вам потрібно додати нову помітну подію, це можливо зробити у Splunk. Перш ніж натиснути кнопку "Зберегти", виберіть: Додати нову дію відповіді> Помітна

Знову ж таки, можна додати деякі налаштування конфігурації за умовчанням для помітної події про те, що всі вони можуть бути змінені, якщо необхідно.

Все, що вам потрібно зробити зараз - це "зберегти". Зауважимо, якщо ви отримаєте повідомлення про те, що макрос недоступний для виконання в пошуку, переконайтеся, що для дозволів програми Anomali ThreatStream встановлено значення global. Ви можете зробити це, перейшовши до: Керування програмами> ThreatStream> Дозволи.

Тепер ви побачите, що будь-які збіги з високим пріоритетом відображатимуться як інформаційні події в інформаційній панелі "Огляд подій".

Команда SOC тепер може призначити ці загрози, використовуючи знайомий робочий процес Enterprise Security[24].

2.4 Боротьба з кіберзлочинністю з аналітикою Splunk Security

Існує багато галузей промисловості, які перебувають у розвитку використання IT: маркетингова аналітика, роздрібна торгівля, служби рекрутингу, аналітика великих даних тощо. Але це хороші спеціалісти, є й інші, які використовують свої глибокі знання про безпеку, хакерство, крекінг, фішинг, щоб скористатися популярністю цих галузей, щоб заробити на цьому гроші. Народився новий вид бізнесу: злочинність як служба (CaaS).

Переваги використання Splunk для боротьби з CaaS описав Маркос Optic Data Engineer «thepandaway.co».

По-перше, доступні функції безпеки продукту. Splunk має дивовижну групу функцій, коли ви шукаєте платформу моніторингу Advanced Security:

Це дозволяє об'єднати всі машинні дані з вашого брандмауера, журнали доступу, мобільні мережі, в одному місці, що дуже важливо для застосування деякого кореляційного аналізу в цих наборах даних.

Це дозволяє робити аналіз розпізнавання образів на основі декількох критеріїв, таких як місце розташування, час доби, критичність даних, тип дії тощо.

Ви можете побачити, що відбувається в режимі реального часу за допомогою добре розробленої панелі інструментів, орієнтованої на ідентифікацію інцидентів безпеки, HTTP-трафік і аналіз, аналіз агента користувача, аналіз розміру трафіку і багато інших корисних для кожного головного оператора безпеки кожного компанії або організації

У ньому є те, що називається «Розширені стійкі загрози», які можна використовувати для аналізу всіх видів загроз у вашій мережі, орієнтованих на розширення шкідливих програм та вибуховий ріст. Це одна з найскладніших проблем глобальної безпеки, тому що дуже важко визначити мережі розповсюдження шкідливих програм, оскільки великі уми, що стоять за такою інфраструктурою, є яскравими і постійно змінюють свою поведінку, використовуючи різні платформи, IP-адреси, провайдери, різні цілі тощо.

По-друге, Splunk накопичила видатну групу експертів з безпеки, щоб щодня привертати інновації в цій галузі. Деякі з них:

Марк Сьюард, старший директор з безпеки та відповідності у Splunk. Джо Голдберг, старший менеджер з маркетингу продуктів у Splunk. Пол Панг, директор з продажів, Азіатсько-Тихоокеанського регіону та Японії в компанії Splunk. Фред Уілмот, міністр нерозумних прогулянок у Splunk, який є експертом у проектуванні та захисті архітектур, мережевої безпеки, керуванні інцидентами, системах CoBIT, PCI, HIPAA та SCADA. Алекс Райц, менеджер і ведучий розробник, програми в Splunk. Джон Топп, старший інженер з продажу в Splunk, GCIA, GCIH, MCSE, ITIL, глобальний експерт з мереж виявлення кіберзагроз.

По-третє, мережа партнерства від Splunk наповнена великими компаніями, такими як Palo Alto Networks, Cloudera, Cisco, RigthScale, Amazon, Microsoft і Vmware. Це величезна перевага для Splunk, тому що ці

партнери мають неймовірну кількість клієнтів, що може бути дуже корисним для бізнесу, і більше компаній і організацій, або як завгодно, вивчає, як поліпшити свою безпеку на своїх платформах, відігравати ключову роль у цих вимогах[25].

Тому Splunk це дійсно потужний інструмент для боротьби з кіберзлочинністю. Ми не будемо використовувати його для цієї цілі в даній роботі, але ми не могли не зазначити такої можливості цієї програми. Адже, якщо ваша ІС представляє інтерес для спеціалістів, то будьте готові, що вона може піддаватися кіберзлочинності.

Висновки до другого розділу

Ми показали основні дія для аналізу стану безпеки ІС. Логування одне з основних методів у захисті інформацію. Відслідковування, керування, збереження аналіз логів значно покращить стан безпеки вашої ІС. В розділі були представлені дії, які необхідні для моніторингу логів систем безпеки і для оперативного реагування на інциденти безпеки, а також перелік можливих джерел і подій, які можуть представляти інтерес для аналізу. Були представленні таблиці, у яких наведено основні події, для яких треба моніторинг логів та ключові слова за якими робити запити SPL. Були наведені приклади для систем Linux і Windows, а також для мережевих пристроїв та веб-сервера.

Було представлено застосування основних елементів програми Splunk. Розглянуто такі режими роботи: представлення показників працездатності і основні пов'язаними з ними KPI, що мають колірний

індикатор і відсортовані за поточним рівнем стану. Таблиці, які дозволяють дізнатися про стан сервісів і значеннях показників ефективності в інтерфейсі схем роботи або бізнес-процесів. У розділі Deep Dives додається історія показників KPI, тобто ми можемо побачити стан системи не тільки зараз, а й кілька годин тому і порівняти результати роботи різних елементів системи в один і той же момент часу або порівняти результати одного сервісу з тим що було день, тиждень або місяць тому. У розділі Multi KPI Alerts можливе створення таких композиційних показників ефективності, в яких можна враховувати вагу впливу кожного фактору на загальну проблему.

Була показана можливість роботи з помітними подіями. Ми можемо керувати подіями, встановлювати певні дії і скрипти на реалізацію події, наприклад, відправляти повідомлення на електронну пошту або в зовнішні системи. Також було підняте питання використання Splunk для захисту від кіберзлочинності.

3 АНАЛІЗ СТАНУ БЕЗПЕКИ METASPLOITABLE 2 ЗА МЕТОДИКОЮ АНАЛІЗУ СТАНУ БЕЗПЕКИ ІС ЗА ДОПОМОГОЮ ПРОГРАМИ SPLUNK

3.1 Обґрунтування вибору ІС.

Перед нами постав вибір ІС для практичного експеременту застосування методики аналізу стану безпеки ІС за допомогою програми Splunk. Нам необхідно використати методику, щоб отримати результати, зробити їх аналіз. Тільки тоді ми зможемо робити висновки про вдалість запропонованої методики.

Чому не можемо взяти першу ІС, яка нам попадеться під руку, наприклад власну ОС? По-перше власна ОС орієнтована на користувацький

режим дуже малий об’єкт у розрізі галузі інформаційної безпеки. Не можна навіть порівняти задачі, які стоять перед захистом користувацької ОС та ІС, які використовуються в промислових масштабах.

По-друге, ми не володіємо інформацією про дійсний стан безпеки власної ОС, отже ми не можемо порівняти отримані результати з дійсними. Тобто ми, якщо використовувати наукову мову, не маємо контрольної групи. Тому було прийнято рішення вибрати сторонню ІС, стан безпеки якої нам відомий. Або вона була проаналізована багатьма спеціалістами, є їх звіти з якими можна ознайомитися. Або, що краще, бо результаті більш надійні, ІС в якій навмисне додані вразливості. В підсумку ми вибрали ІС Metasploitable другої версії.

Це віртуальна машини, спеціально спроектована на максимальну вразливість для тренування, тестів експлойтів і навчання новачків. На відміну від інших вразливих віртуальних машин, Metasploitable фокусується на вразливості в операційній системі Linux і мережевих сервісах, а не на окремих додатках.

Metasploitable 2 - щось на зразок боксерської груші для роботи «пентестеров» і використання програм на зразок Metasploit і Nmap. У ній відкриті всі порти і присутні всі відомі уразливості, деякі з яких ви можете зустріти в реальному житті на реальних системах[26].

Основні відомості про віртуальну машину Metasploitable 2:

- Він працює під управлінням Linux 2.6.9 - 2.6.33 в якості операційної системи.
- Ім'я сервера METASPLOITABLE.
- Доступно 35 облікових записів користувачів.
- Msfadmin - це обліковий запис адміністратора.
- У пароля облікового запису адміністратора msfadmin немає терміну дії.
- Ми знаємо, які служби працюють, версії цих служб і на якому порту вони слухають.

- На Metasploitable машині працюють веб-сервер і SQL-сервер[27].

Отже, вибрана ІС має відомий стан безпеки і ми зможемо порівняти отримані результати, отримати ясну картину про успішність запропонованої методики аналізу стану безпеки ІС за допомогою програми Splunk. Саме був зроблений вибір на користь даної ОС. Також слід зазначити, що дана ОС є офіційним продуктом, тому має офіційний сайт, на якому є документація та гайд по використанню ОС Metasploitable 2. Також є велике ком'юніті, яке може допомогти у вирішені деяких питань та задач.

3.2 Установка програми Splunk та ОС Metasploitable 2

3.2.1 Установка ОС Metasploitable 2

Для установки потрібної нам ОС завантажимо її з офіційного сайту[28]. (див. рис. 3.1)

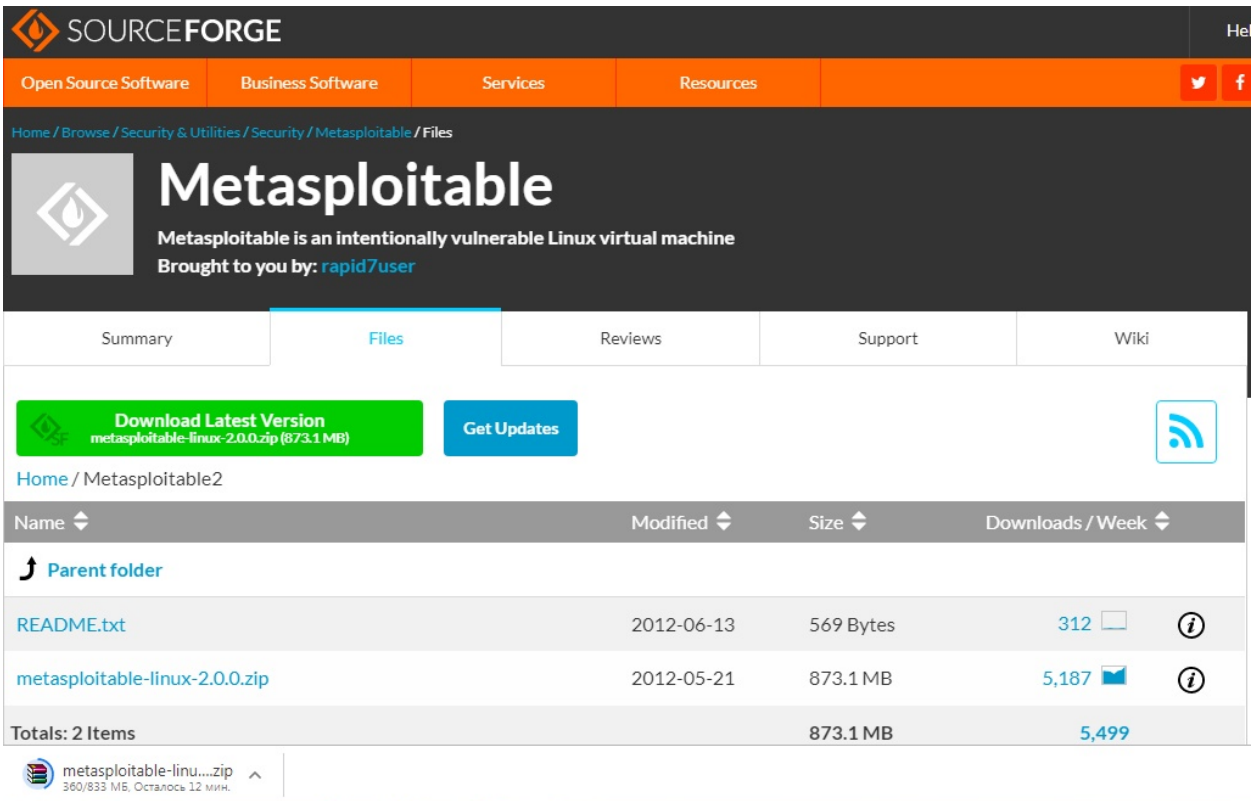

Рисунок 3.1 – завантаження ОС Metasploitable 2

Коли завантаження завершено, розархівіруємо завантажену папку. Ми вже маємо установлену програму VMWare, вона нам була потрібна для курсу Захист ОС 2. Відкриваємо програму тиснем файл>відкрити, і вибираємо завантажену папку і в ній файл з розширенням .vmx. (див. рис. 3.2)

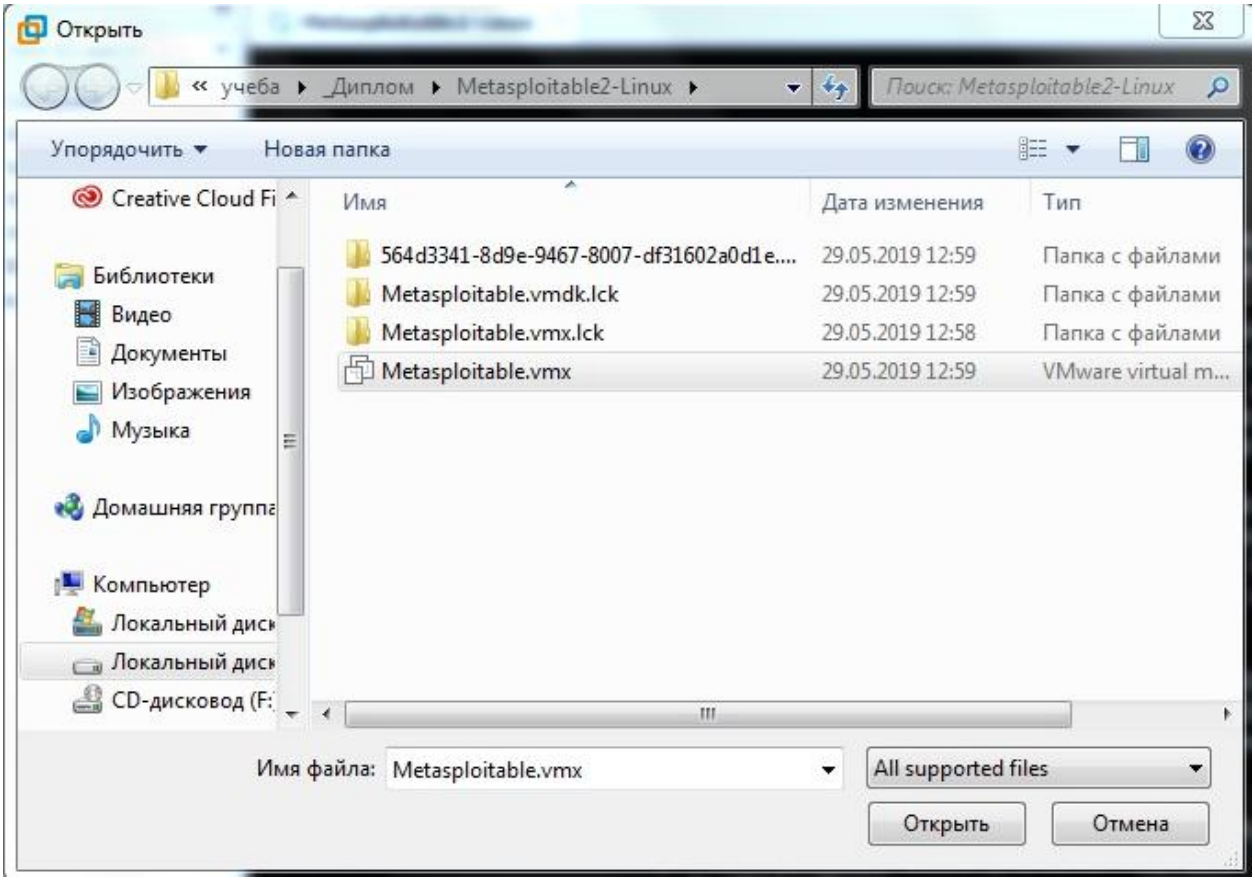

Рисунок 3.2 – Відкриття файлу Metasploitable.vmx

Далі треба ввести ім’я адміністратора msfadmin і його пароль. (див. рис. 3.3)

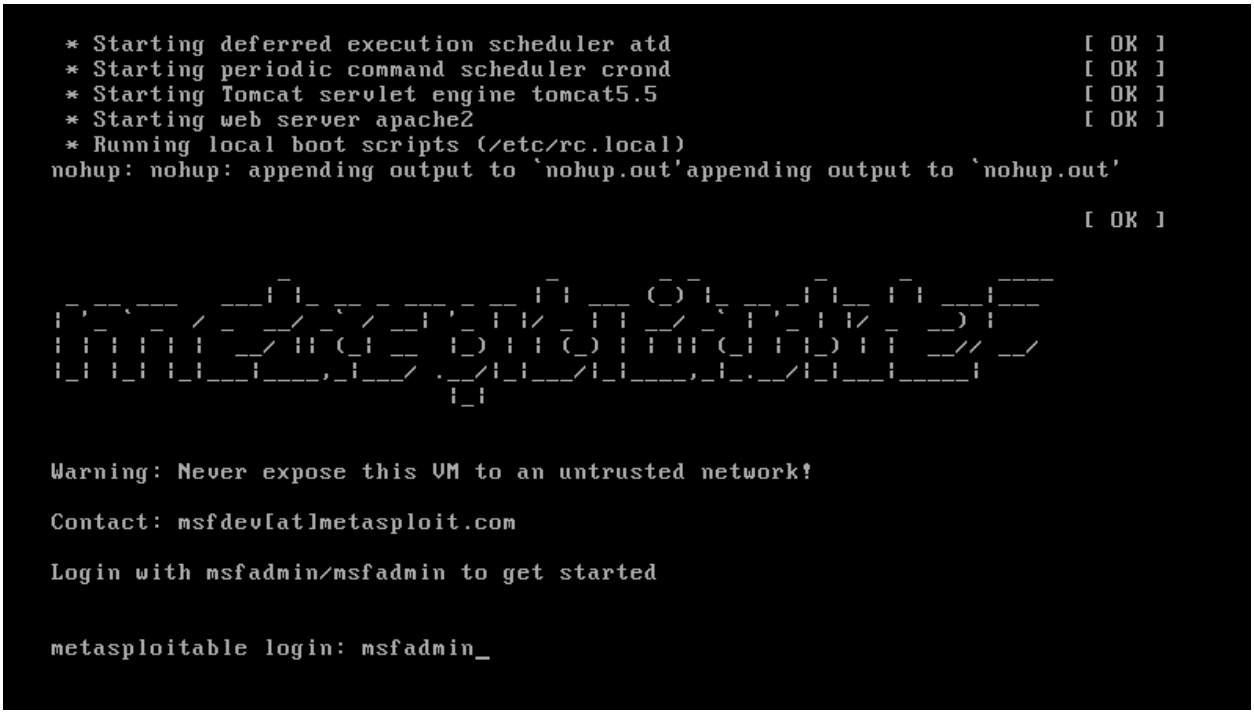

Рисунок 3.3 – адміністратор

Після цього установку завершено. Тепер ми можемо перейти до установки програми Splunk.

3.2.1 Установка програми Splunk

Тепер нам потрібно установити саму програму Splunk, для цього завантажимо програму з офіційного сайту[4]. (див. рис. 3.4)

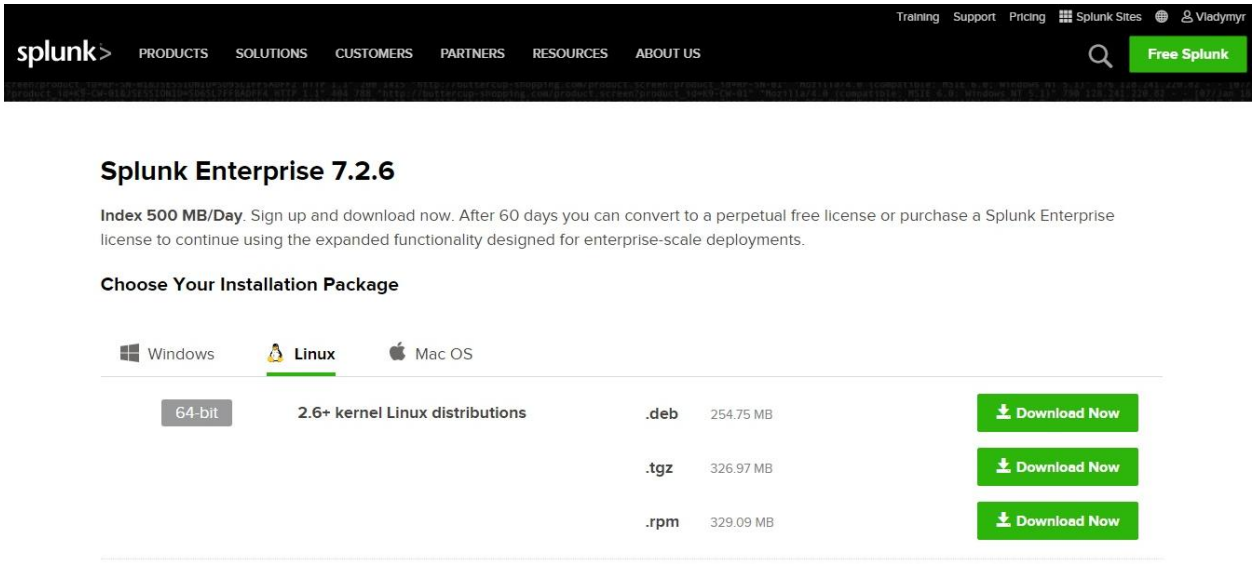

Рисунок 3.4 – Сайт Splunk

Далі у консолі введемо команду:

tar xvzf splunk_package_name.tgz -C /opt

Установка почнеться. (див. рис. 3.5)

Рисунок 3.5 – Установка Splunk

Тепер залишилося лише погодитися з ліцензійним угодою. Вести логін користувача та пароль, під яким ми будемо виконувати аналіз стану безпеки ІС, та натиснути старт. І нарешті, ввійти в нашого користувача і ми можемо починати. (див. рис. 3.6)

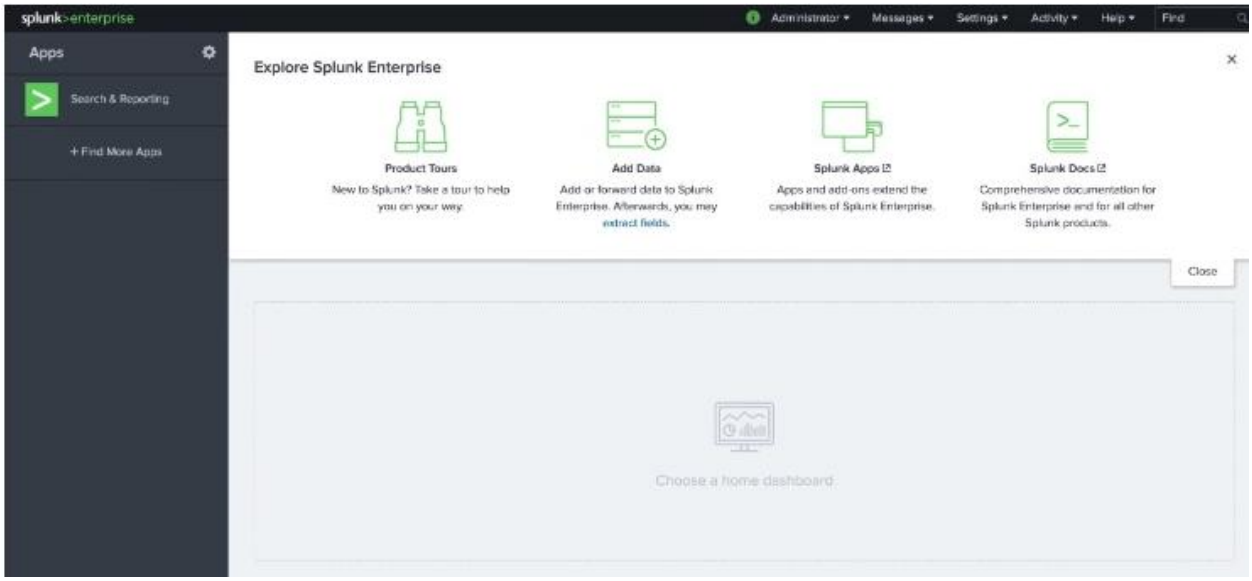

Рисунок 3.6 - Splunk

3.3 Аналіз стану безпеки Metasploitable 2 за методикою аналізу стану безпеки ІС за допомогою програми Splunk

3.3.1 Логування за допомогою Splunk

На нашій ОС логування не налаштоване, тому всі логи будуть зберігатися за замовченням у / var / log. Проскануємо цю директорію за допомогою Splunk. (див. рис. 3.7)

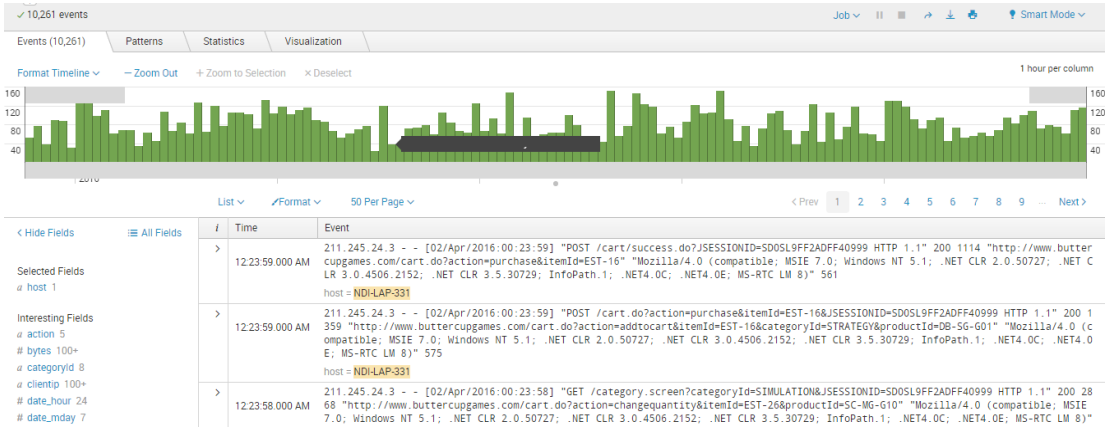

Рисунок 3.7 – Логи

Ми отримали 10 261 лог, з моменту установки ОС пройшло 4 год 47 хв, тому можемо порахувати скільки логів ми будемо отримувати за одну добу, якщо тенденція буде зберігатися. Також порахуємо кількість логів за хвилину, а також подивимося скільки логів ми отримали кожної категорії: emerg, alert, crit, err, warning, notice, info, debug.

За допомогою Splunk ми налаштуємо зберігання логів в окремі файли, в залежності від категорії та джерела. (див. табл. 3.1)

Таблиця 3.1 – Файли логів

Файл	**Категорія**	**Джерело**
emerg.log	emerg	Усі
alert.log	alert	Усі
crit.log	crit	Усі
err_kern.log	err	Ядро
err_user.log	err	Користувач
err_security.log	err	Системи безпеки
err.log	err	Усі, крім ядра, користувача і систем безпеки
Warning_kern.log	warning	Ядро
Warning_user.log	warning	Користувач

Продовження таблиці 3.1

Warning.log	warning	Усі, крім ядра, користувача і систем безпеки
Warning_security.log	warning	Системи безпеки
Notice.log	notice	Усі
Info.log	info	Усі
Debug.log	debug	Усі

Також слід зазначити, що за допомогою програми Splunk ми можемо налаштувати повідомлення про важливі логи, наприклад перших трьох категорій на електрону пошту або в телеграм. Але так, як ми робимо аналіз стану безпеки, а не налаштовуємо захист для майбутнього користування, ми цього робити не будемо.

3.3.2 Застосування основних елементів Splunk IT Service Intelligence

1) Service Analyzer

Завдяки Service Analyzer побачимо завантаженість системи. У структурі плитка (див. рис. 3.8) та у деревовидній структурі (див. рис. 3.9).

Слід зазначити, що система мало завантажена, адже ми не виконуємо ніяких дій на ОС, не виходимо в інтернет тощо.

Рисунок 3.8 – Плитка

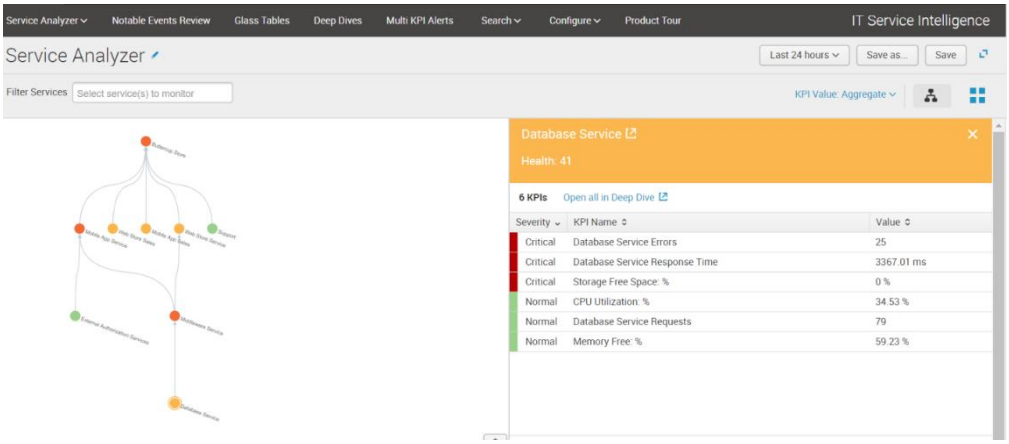

Рисунок 3.9 – Деревовидна структура

2) Deep Dives

Завдяки Deep Dives подивимося показники KPI для деяких елементів системи за проміжок часу. (див. рис. 3.10).

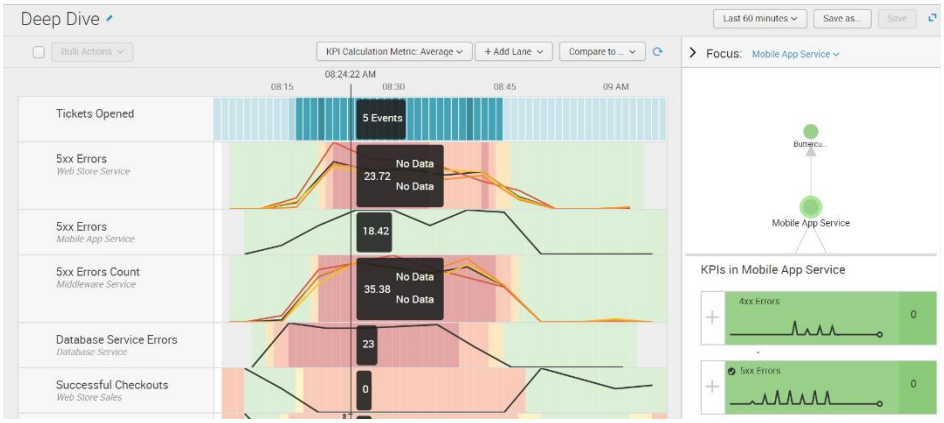

Рисунок 3.10 - Deep Dives

3) Multi KPI Alerts

Завдяки Multi KPI Alerts ми можемо створити об’єднані повідомлення, коли дві системи, які пов’язанні мають проблеми. (див. рис. 3.11).

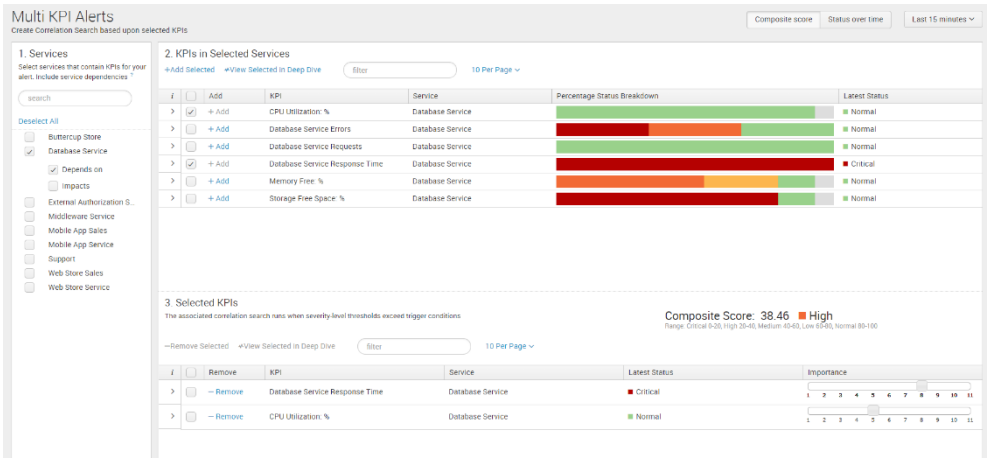

Рисунок 3.11 - Multi KPI Alerts

3.3.3 Помітні події у Splunk

1) Notable Events Review

Завдяки Notable Events Review можемо одразу просканувати систему на помітні події без зайвих складних дій.

Отримали деякі цікаві результаті, про які поговоримо в наступному підрозділі.

2) Кореляційний пошук

У цьому прикладі ми просто скопіюємо один з пошуків з програми ThreatStream, яке з високим ступенем достовірності оповіщає на основі високо пріоритетних збігів індикаторів APT, C2 або шкідливих програм, і перетворимо його в кореляційний пошук. (див. рис. 3.13).

Ми отримали аж два повідомлення про загрози, хоча ми не працювали в інтернеті, окрім завантаження програми Splunk, не завантажували неперевірених програм та не переходили на не перевірені сайти. (див. рис. 3.14)

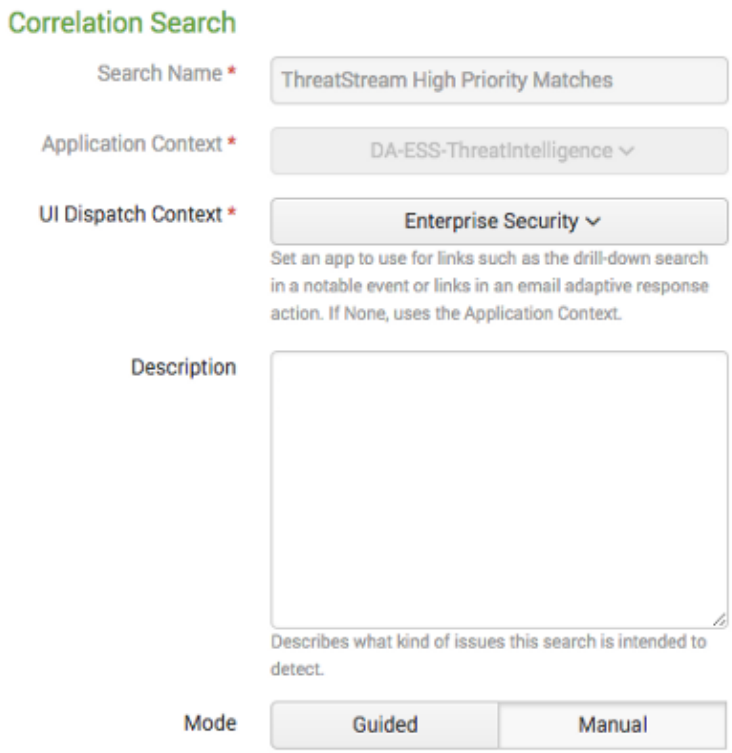

Рисунок 3.13 – кореляційний пошук

	Indicator	sourcetype	Victim	Age	Indicator Source	iType	Confidence	Severity	ts_type
08:30:00	221.239.8.178	cisco:sourcefire	10.161.146.110	19	Jigsaw Professional	mal_ip	89	very-high	ip
08:50:00	193.238.37.183	cisco:sourcefire	10.176.221.247	23	Symantec DeepSight Advanced IP Reputation Malware iSIGHT Partners Cyber Crime	bot_ip mal_ip	100 85	low very-high	ip

Рисунок 3.14 – Результат кореляційного пошуку

3)Додавання помітної події

Тепер зробимо так, щоб ми бачили помітні події пов’язанні з цими загрозами, без спеціальної перевірки. (див. рис. 3.15)

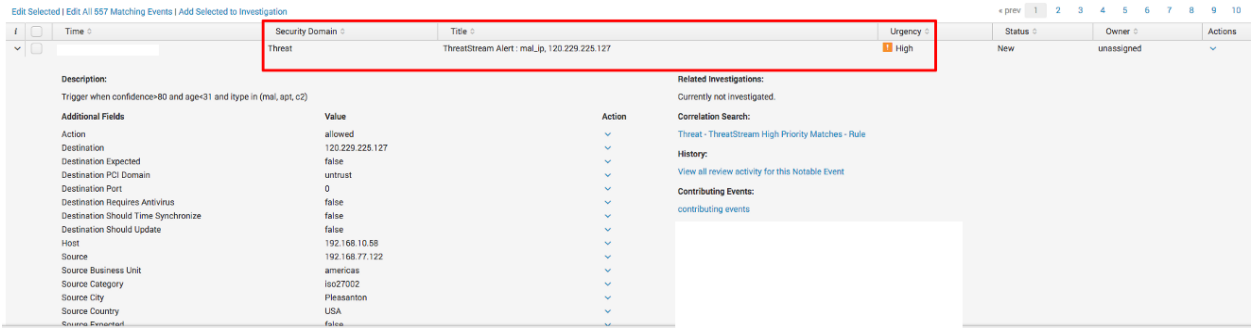

Рисунок 3.15 – Додавання помітної події

3.4 Аналіз результатів

Отже, за 4 год 47 хв ми отримали 10 261 логи. Порахували приблизну кількість логів на добу - отримали результат 51 484. Також порахували приблизну середню кількість за хвилину – отримали результат 36. Також для порівняння зазначимо, що на власній ОС ми маємо менше 100 логів на добу, а за хвилину, що ми спостерігали отримали одне повідомлення про аудит успіху. Тепер ми можемо для представлення картини стану безпеки розподілити логи за категорією, для того щоб побачити скільки маємо небезпечних повідомлень. (див. табл. 3.2)

Таблиця 3.2 – Логи за категоріями

Категорія	**Кількість**
emerg	1
alert	12
crit	113
Err	657
Warning	1 834
Notice	2 348
Info	2 457
Debug	2 839

Що можна виділити маємо 1 повідомлення категорії emerg, і дійсно один раз система власноруч припинила роботу.

Також маємо 12 і 113 помилок категорії alert і crit відповідно, що також дуже погано. На такій системі не бажано працювати звичайному користувачеві, вже не кажучи про промисловість або бізнес.

Відповідно ми отримали ще приблизно дві с половинної тисячі повідомлень категорій Err і Warning, що не є небезпечними повідомленнями для роботи ІС.

Також ми налаштували зберігання логів в окремі файли, тепер можемо не фільтрувати усі логи, а просто подивитися потрібний файл. Також слід зазначити, що за допомогою програми Splunk ми можемо налаштувати повідомлення про важливі логи, наприклад перших трьох категорій на електрону пошту або в телеграм. Але так, як ми робимо аналіз стану безпеки, а не налаштовуємо захист для майбутнього користування, ми цього робити не будемо.

Елементи Splunk IT Service Intelligence, якщо підсумовувати, показали нам легку завантаженість системи. Для нашої ОС в даному випадку, ми отримали розуміння масштабів. Той стан безпеки, який ми отримаємо в результаті аналізу стану безпеки, це не максимальна загорза від того, що буде відбуватися з системою, якщо її навантажити.

Які бувають помітні події:

- Один з KPI, якщо він перевищує заданий поріг;
- Результат роботи Multi KPI Alerts, який генерує попередження, засноване на стані кількох KPI;
- Результат кореляційного пошуку, який шукає відносини між точками даних.

Отримати перші два варіанти ми не могли, тому будемо розглядати тільки третій варіант. Коли налаштували кореляційний пошук на загрозливі програми, ми отримали дві помітні події. Ось що написано в пункті Indicator Source помітної події - Malware і Cyber Crime.

Звичайно це свідчить про незахищеність системи, адже ми отримали аж два повідомлення про загрози, хоча ми не працювали в інтернеті, окрім завантаження програми Splunk, не завантажували неперевірених програм та не переходили на неперевірені сайти.

В підсумку ми вирішили оцінити стан кожного пункту і системи в цілому. Зробили ми це у відсотках, де 0% - це ідеально захищена система, ймовірність загрози якій неможлива, а 100% відсотків – це абсолютно

незахищена система. І представили все у вигляді кругової діаграми(див. рис. 3.16):

Рисунок 3.16 – Стан Безпеки

Отже можемо впевнено зазначити, що система дуже вразлива, і не можна працювати з нею, або будувати на ній ІС.

Висновки до третього розділу

Отже ми проаналізували стан безпеки ОС Metasploitable 2 за допомогою програми Splunk. Для цього було здійснено журналювання логів, використання елементів Splunk IT Service Intelligence, ми розглянули помітні події і зробили висновки щодо загального стану безпеки ОС Metasploitable 2.

Під час огляду логів ОС ми відзначили повідомлення високої категорії важливості. Також ми отримали велику кількість логів - 10 261. Ми додали правила журналювання логів, виділили повідомленя від певних джерел та певних категорії в окремі файли.

Елементи Splunk IT Service Intelligence: Services і KPIs показують, які сервіси в даний момент працюють нормально, а які мають відхилення. Glass Tables дозволяють згрупувати показники за специфічними групами і наочно візуалізувати їх. Deep Dives дозволяє порівнювати стан показників в часі і визначати з якого джерела почалася та чи інша проблема. Multu-KPI Alerts виявляють якісь конкретні важливі події і дозволяють керувати ними.

Коли налаштували кореляційний пошук на загрозливі програми, ми отримали дві помітні події. Ось що написано в пункті Indicator Source помітної події - Malware і Cyber Crime.

Звичайно це свідчить про незахищеність системи, адже ми отримали аж два повідомлення про загрози, хоча ми не працювали в інтернеті, окрім завантаження програми Splunk, не завантажували неперевірених програм та не переходили на неперевірені сайти.

В підсумку ми вирішили оцінити стан кожного пункту і системи в цілому. Зробили ми це у відсотках, де 0% - це ідеально захищена система, ймовірність загрози якій неможлива, а 100% відсотків – це абсолютно незахищена система. І представили все у вигляді кругової діаграми(див. рис. 3.16)

Отже можемо впевнено зазначити, що система дуже вразлива, і не можна працювати з нею, або будувати на ній ІС.

ВИСНОВКИ

Проблема якісного аналізу безпеки дуже актуальна у сучасній Україні, оскільки ІС стає все більше. Успішність роботи системи напряму залежить від стану безпеки ІС. Splunk одна з передових програм в аналізі безпеки, вона має дуже великий набір можливостей і з успіхом використовується по всьому світу. В Україні їй приділено мало уваги, але вона набирає популярності і в майбутньому може зайняти лідерство.

Через те, що Splunk почали використовувати в Україні відносно нещодавно, існує проблема методології. Матеріалів з використанням Splunk дуже мало, і здебільшого це дуже вузькоспеціалізовані гайди або рішення однієї проблеми або задачі з використання Splunk. В цій роботі ми розглянули програму Splunk, як інструмент аналізу стану безпеки ІС, і ми можемо зазначити, що не існує жодної методики з комплексного аналізу стану безпеки ІС. Саме цю проблеми було прийнято рішення вирішити у даній роботі.

В першому розділі було розглянуто роль SIEM-систем у захисті ІС. У разі успішного впровадження та експлуатації SIEM-системи буде здійснена кореляція та обробка подій безпеки. Також дає можливість побудови систем та центрів моніторингу та реагування, автоматизацію процесів виявлення загроз та аномалій, автоматизацію процесів реєстрації та контролю інцидентів, з подальшою можливістю їх розслідування. Дозволяє реагувати на загрози, що виникають, в режимі реального часу [2].

В Україні в сьогоднішніх економічних та політичних умовах ринок SIEM розвивається повільніше, ніж за кордоном. Не всі світові лідери мають представництва в нашій країні. Хоча спостерігається позитивна тенденція в розвитку.

Було детально розглянуто програму Splunk. Вона дозволяє швидко отримати результат від використання. Splunk є універсальною платформою для машинних даних, яка забезпечує комплексний збір даних, їх обробку та аналіз. Splunk дозволяє аналізувати інциденти для визначення обставин і масштабів інциденту. Система дозволяє здійснювати пошук як за даними в реальному часі, так і за архівними даними, на основі результатів пошуку Splunk дає можливість: аналізувати отримані результати за допомогою засобів візуалізації, формувати звіти і попередження, створювати систему моніторингу та повідомлень в реальному часі[3].

Також була піднята проблему методології SIEM-систем та зокрема програми Splunk. Ми маємо достатньо інформації про програму Splunk, але немає комплексних методик для вирішення загальних проблем. Наприклад, методики аналізу стану безпеки ІС.

В другому розділі була описана методика аналізу стану безпеки ІС за допомогою програми Splunk. Ми показали основні дія для аналізу стану безпеки ІС. Логування одне з основних методів у захисті інформацію. Відслідковування, керування, збереження аналіз логів значно покращить стан безпеки вашої ІС. В розділі були представлені дії, які необхідні для моніторингу логів систем безпеки і для оперативного реагування на інциденти безпеки, а також перелік можливих джерел і подій, які можуть представляти інтерес для аналізу. Були представленні таблиці, у яких наведено основні події, для яких треба моніторинг логів та ключові слова за якими робити запити SPL.

Було представлено застосування основних елементів програми Splunk. Розглянуто такі режими роботи: представлення показників працездатності і основні пов'язаними з ними KPI, що мають колірний індикатор і відсортовані за поточним рівнем стану. Таблиці, які дозволяють дізнатися про стан сервісів і значеннях показників ефективності в інтерфейсі схем роботи або бізнес-процесів. У розділі Deep Dives додається історія показників KPI, тобто ми можемо побачити стан системи не тільки

зараз, а й кілька годин тому і порівняти результати роботи різних елементів системи в один і той же момент часу або порівняти результати одного сервісу з тим що було день, тиждень або місяць тому. У розділі Multi KPI Alerts можливе створення таких композиційних показників ефективності, в яких можна враховувати вагу впливу кожного фактору на загальну проблему.

Була показана можливість роботи з помітними подіями. Ми можемо керувати подіями, встановлювати певні дії і скрипти на реалізацію події, наприклад, відправляти повідомлення на електронну пошту або в зовнішні системи. Також було підняте питання використання Splunk для захисту від кіберзлочинності.

В третьому розділі ми проаналізували стан безпеки ОС Metasploitable 2 за допомогою програми Splunk. Для цього було здійснено журналювання логів, використання елементів Splunk IT Service Intelligence, ми розглянули помітні події і зробили висновки щодо загального стану безпеки ОС Metasploitable 2.

Під час огляду логів ОС ми відзначили повідомлення високої категорії важливості. Також ми отримали велику кількість логів - 10 261. Ми додали правила журналювання логів, виділили повідомленя від певних джерел та певних категорії в окремі файли.

Елементи Splunk IT Service Intelligence: Services і KPIs показують, які сервіси в даний момент працюють нормально, а які мають відхилення. Glass Tables дозволяють згрупувати показники за специфічними групами і наочно візуалізувати їх. Deep Dives дозволяє порівнювати стан показників в часі і визначати з якого джерела почалася та чи інша проблема. Multu-KPI Alerts виявляють якісь конкретні важливі події і дозволяють керувати ними.

Коли налаштували кореляційний пошук на загрозливі програми, ми отримали дві помітні події. Ось що написано в пункті Indicator Source помітної події - Malware і Cyber Crime.

В підсумку ми вирішили оцінити стан кожного пункту і системи в цілому. Зробили ми це у відсотках, де 0% - це ідеально захищена система, ймовірність загрози якій неможлива, а 100% відсотків – це абсолютно незахищена система. І представили все у вигляді кругової діаграми(див. рис. 3.16)

Отже можемо впевнено зазначити, що система дуже вразлива, і не можна працювати з нею, або будувати на ній ІС.

Мета роботи удосконалити методи аналізу безпеки ІС, шляхом розробки методики аналізу стану безпеки за допомогою програми Splunk. Мета роботи досягнута. Також перед нами стояли завдання: Дослідити методи аналізу безпеки ІС за допомогою програми Splunk. Розробити методику аналізу безпеки ІС за допомогою програми Splunk. Зробити аналіз стану безпеки Metasploitable 2 за допомогою програми Splunk, для підтвердження успішності запропонованої методики.

Ми впевнені, що в майбутньому SIEM-системи будуть невід’ємною частиною безпеки будь-якої ІС. Зараз архітектура ІС стає все більш складною. Раніше всі функції, які повинна виконувати ІС, повинна була містити ці функції. Але зараз часто використовуються додаткові модулі або навіть гібридні хмари, як додаткове програмне забезпечення. А вони в свою чергу вже містять власну SIEM-систем, тому нашій системі доведеться приєднатися до неї, для того щоб обмінюватися даними. Тому в майбутньому очікується розвиток гібридних SIEM-систем.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Вікіпедія: SIEM [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/SIEM - 27.07.2018 р.
2. Огляд світового ринку SIEM-систем [Електронний ресурс] / А. Саприкіна. – Режим доступу: https://www.anti-malware.ru/analytics/Market_Analysis/overview-global-and-russian-market-siem#part1- 23.08.2017 р.
3. Вікіпедія: Splunk [Електронний ресурс] – Режим доступу: https://ru.wikipedia.org/wiki/Splunk - 13.09.2018 р.
4. Офіційний сайт Splunk [Електронний ресурс] – Режим доступу: https://www.splunk.com/ - 2005 р.
5. Аналітика роботи додатків [Електронний ресурс] Ю. Корольова – Режим доступу: https://habr.com/ru/company/tssolution/blog/417909/ - 22.06.2018 р.
6. Аналітика подій безпеки [Електронний ресурс] Ю. Корольова – Режим доступу: https://habr.com/ru/company/tssolution/blog/417909/ - 08.08.2018 р.
7. Офіційний сайт ARC [Електронний ресурс] – Режим доступу: https://habr.com/ru/company/tssolution/blog/417909/ - 2008 р.
8. Інтернет речей та промислові дані [Електронний ресурс] Ю. Корольова – Режим доступу: https://habr.com/ru/company/tssolution/blog/420021/ - 14.08.2018 р.
9. Splunk - загальний опис платформи, базові особливості установки і архітектури [Електронний ресурс] А. Кулаков – Режим доступу: https://habr.com/ru/company/tssolution/blog/323814/ - 14.03.2018 р.

10. The Coolest Big Data Management And Integration Software Of The 2019 Big Data 100 [Електронний ресурс] Р. Уайтинг– Режим доступу: https://www.crn.com/slide-shows/storage/the-coolest-big-data-management-and-integration-software-of-the-2019-big-data-100/ - 01.05.2019 р.
11. Top Companies 2019: Where the U.S. wants to work now [Електронний ресурс] Д. Рот – Режим доступу: https://www.linkedin.com/pulse/top-companies-2019-where-us-wants-work-now-daniel-roth/ - 03.04.2019 р.
12. Best Software Products 2019 [Електронний ресурс] – Режим доступу: https://www.g2.com/best-software-companies/top-products - 13.06.2019 р.
13. RRC і Splunk відчиняють двері [Електронний ресурс] А. Фролов – Режим доступу: https://security-news.today/rrc-i-splunk-otkryvayut-dveri/ - 22.07.2016
14. SmartTender [Електронний ресурс] – Режим доступу: https://smarttender.biz/publichni-zakupivli-prozorro/4418533/ - 2018 р.
15. Derek Mock, Splunk Operational Intelligence Cookbook [Текст]: Josh Diakun, Paul R. Johnson, Derek Mock. – M.: Packt Publishing, 2016.
16. Vincent Bumgarner, Implementing Splunk Big Data Reporting and Development for Operational Intelligence [Текст]: Vincent Bumgarner. – M.: Packt Publishing, 2013.
17. Manuals Splunk Enterprise [Електронний ресурс] – Режим доступу: https://docs.splunk.com/Documentation/Splunk/ - 2005 р.
18. Splunk. Підбірка корисних матеріалів від TS Solution [Електронний ресурс] А. Кулаков – Режим доступу: https://docs.splunk.com/Documentation/Splunk/ - 17.05.2018 р.
19. Чек-лист з аналізу логів подій безпеки [Електронний ресурс] Ю. Корольова – Режим доступу: https://habr.com/ru/company/tssolution/blog/416313/ - 06.06.2018 р.
20. Моніторинг ефективності роботи IT систем за допомогою Splunk IT Service Intelligence [Електронний ресурс] Ю. Корольова – Режим доступу: https://habr.com/ru/company/tssolution/blog/416313/ - 20.02.2018

21. Форум anomali.com [Електронний ресурс] – Режим доступу: https://forum.anomali.com/ - 2010 р.
22. Splunk documentation: Notable Event [Електронний ресурс] – Режим доступу: https://docs.splunk.com/Splexicon:Notableevent – 2005 р.
23. Splunk documentation: Correlation Search [Електронний ресурс] – Режим доступу: https://docs.splunk.com/Splexicon: Correlationsearch – 2005 р.
24. ThreatStream Matches As Notable Events in Splunk? Here's How… [Електронний ресурс] David Greenwood – Режим доступу: https://medium.com/@himynamesdave/threatstream-matches-as-notable-events-in-splunk-heres-how-70fa09a76cb2 – 17.08.2017 р.
25. Fighting Cybercrime with Splunk Security Analytics [Електронний ресурс] Marcos Ortiz – Режим доступу: https://medium.com/a-data-driven-guy/fighting-cybercrime-with-splunk-security-analytics-bb6eb33f9d6d – 12.05.2013 р.
26. Metasploitable 2: віртуальна машина Linux для тренування [Електронний ресурс] А. Алізар – Режим доступу: https://xakep.ru/2012/06/15/58852/– 12.06.2012 р.
27. Metasploitable 2 vulnerability assessment [Електронний ресурс] – Режим доступу: https://www.hackingtutorials.org/metasploit-tutorials/metasploitable-2-vulnerability-assessment – 05.06.2016 р.
28. Metasploitable Download [Електронний ресурс] – Режим доступу: https://sourceforge.net/projects/metasploitable/files/Metasploitable2/ – 13.06.2016 р.
29. Основи роботи з Splunk Enterprise (Snort + OSSEC) [Електронний ресурс] – Режим доступу: https://defcon.ru/network-security/3585/ – 29.09.2016 р.