ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ФУНКЦІОНУВАННЯ БОТІВ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ НА БАЗІ SPLUNK»

Виконав студент 6 курсу, групи БСЗМ-61
спеціальності 125 Кібербезпека
освітньо-професійної програми«Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)

Воробей В.В.
(прізвище та ініціали)

Керівник Гахов С.О.
(прізвище та ініціали)

Рецензент
(прізвище та ініціали)

Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ - 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

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

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

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

Вороб’ю Віктору Вікторовичу
(прізвище, ім’я, по батькові)

1. Тема магістерської роботи: «Технологія виявлення функціонування ботів в Інформаційній системі організації на базі Splunk»

керівник магістерської роботи Гахов Сергій Олександрович, к.військ.н., доцент
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «12» жовтня 2022 року №122.

2. Строк подання студентом магістерської роботи 15.12.2022 р.

3. Вихідні дані до магістерської роботи
Інформаційна система організації;
Виявлення функціонування ботів;
Наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз проблеми виявлення функціонування ботів в інформаційній системі організації.
2. Аналіз методів та засобів виявлення функціонування ботів в інформаційних системах організації на базі Splunk.
3. Варіант технології виявлення функціонуваннння ботів в інформаційній системі організації на базі Splunk.
4. Варіант технології виявлення функціонування ботів в інформаційній системі організації.

5. Перелік графічного матеріалу

1. Тема магістерської роботи.

2. Об’єкт, предмет, мета та наукові завдання дослідження.

3. Дослідження проблеми функціонування ботів в ІС організації.

4. Аналіз методів та засобів виявлення функціонування ботів в інформаційній системі організації.

5. Призначення та архітектува рішення Splunk Enterprise.

6. Призначення та архітектура рішення Splunk Entrprise Security.

7. Варіант технології виявлення функціонування ботів в інформаційній системі організації на базі Splunk.

8. Рекомендації щодо застосування технології виявлення функціонування ботів в інформаційній системі організації.

6. Дата видачі завдання 26.09.2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів магістерської роботи	Строк виконання етапів магістерської роботи	Примітка
1.	Визначення актуальності проблеми захисту від ботів інформаційних систем.	26.09.2022 р.	
2.	Аналіз наукової та технічної літератури з питань теми магістерської роботи.	30.09.2022 р.	
3.	Аналіз методів та засобів виявлення функціонування ботів в інформаційній системі організації.	10.10.2022 р.	
4.	Розроблення варіанту технології виявлення функціонування ботів в інформаційній системі організації.	10.11.2022 р.	
5.	Розроблення рекомендацій щодо застосування технології виявлення функціонування ботів в інформаційній системі організації.	30.112022 р.	
6.	Оформлення результатів дослідження. Проходження плагіату	14.11.2022 р.	
7.	Підготовка доповіді до захисту.	15.12.2022 р.	

Студент Воробей В.В.
(підпис) прізвище та ініціали

Керівник магістерської роботи Гахов С.О.
(підпис) прізвище та ініціали

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ

ЩОДО ЗАХИСТУ МАГІСТЕРСЬКОЇ РОБОТИ

Направляється студент Воробей В.В. до захисту магістерської роботи
(прізвище та ініціали)
спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Технологія виявлення функціонування ботів в інформаційній системі організації на базі Splunk».

Магістерська робота і рецензія додаються.

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

Довідка про успішність

Воробей В.В. за період навчання в інституті
(прізвище та ініціали студента)
ННІЗІ з 2021 року по 2023 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.

Секретар інституту _____ БреславськаТ.В
(підпис) (прізвище та ініціали)

Висновок керівника магістерськоїї роботи

Студент ***Воробей В.В.*** обрав тему роботи, метою якої було дослідити зміст технології виявлення функціонування ботів в інформаційній системі організації на базі Splunk. Перелік використаних джерел свідчить про вміння магістром розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання магістерської роботи Воробей В.В. показав відмінну теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.
Все це дозволяє оцінити виконану магістерську роботу студента Вороб'я Віктора Вікторовича на оцінку «відмінно» та присвоїти йому кваліфікацію магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Керівник магістерської роботи _____ Гахов С.О.
(підпис) (прізвище та ініціали)
"____" _____ 2022 року

Висновок кафедри про магістерську роботу

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

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

ВІДГУК РЕЦЕНЗЕНТА

на магістерську роботу

студента Вороб'я Віктора Вікторовича
на тему: «Технологія виявлення функціонування ботів в інформаційній системі організації на базі Splunk»

Актуальність:
Сучасна організація не може функціонувати без кінцевого обладнання, як інтерфейс взаємодії людини з інформаційною системою. Оскільки з кінцевим обладнанням найчастіше працюють люди, то дедалі частіше зловмисники націлюються на них з метою вчинення бот інфікування. Реалізація технології виявлення функціонування ботів в інформаційній системі організації створює умови забезпечення багатьох сучасних функцій захисту. Тому тема магістерської роботи є актуальною та своєчасною.

Позитивні сторони:

1. На основі проведеного аналізу, в роботі встановлено зміст проблеми функціонування ботів в інформаційній системі організації, визначено мета та завдання виявлення функціонування ботів в інформаційній системі організації.
2. Досліджено методи та засоби виявлення функціонування ботів в інформаційній системі організації.
3. Запропоновано варіант технології виявлення функціонування ботів в інформаційній системі організації на базі рішення Splunk та рекомендації щодо її застосування.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно..

Недоліки:

1. У магістерській роботі доцільно було б використовувати в якості джерел більше підручників та посібників, наукових статей.

Висновок: Враховуючи недоліки, магістерська робота заслуговує оцінку «**відмінно»**, а студент **Воробей Віктор Вікторович** - присвоєння кваліфікації магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека..

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

Підпис рецензента (_____)

_____

РЕФЕРАТ

Текстова частина магістерської роботи: 51 сторінку, 18 рисунків, 4 таблиці, 15 джерел.

Об'єкт дослідження – виявлення функціонування ботів в інформаційній системі організації.

Предмет дослідження – технологія виявлення функціонування ботів в інформаційній системі організації на базі Splunk.

Мета роботи – запропонувати технологію виявлення функціонування ботів в інформаційній системі організації та розробити рекомендацію щодо її застосування.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання технології виявлення функціонування ботів в інформаційній системі організації.

В роботі проаналізовано проблему функціонування ботів в інформаційній системі організації та визначено мета та завдання виявлення функціонування ботів в інформаційній системі організації. Проаналізовано існуючі технологій виявлення функціонування ботів в інформаційній системі організаціях.

Досліджено методи та засоби виявлення функціонування ботів в інформаційній системі організації на базі Splunk. Визначено призначення, основні функції, склад та архітектуру рішення Splunk..

На основі досліджень проведених в роботі розроблено варіант технології виявлення функціонування ботів в інформаційній системі організації та рекомендації щодо її застосування на підприємстві.

Галузь використання – кібербезпека корпоративної інформаційної системи.

ІНФОРМАЦІЙНА СИСТЕМА, КІБЕРБЕЗПЕКА, БОТ, ТЕХНОЛОГІЯ ВИЯВЛЕННЯ БОТІВ В ІНФОРМАЦІЙНІЙ СИСТЕМІ

ABSTRACT

Master’s thesis: 51 pages, 18 figures, 4 tables, 15 sources.

Object of research – is to identify the functioning of bots in the organization's information system.

Subject of research – is the technology for detecting the functioning of bots in the organization's information system based on Splunk..

The aim of research – is to propose a technology for detecting the functioning of bots in the organization's information system and to develop a recommendation for its use.

Research methods – study of the literature on this topic, analysis of operating documentation, international standards and their comparison, modeling of technology for detecting the functioning of bots in the organization's information system.

The paper analyzes the problem of the functioning of bots in the organization's information system and defines the purpose and task of detecting the functioning of bots in the organization's information system. Existing technologies for detecting the functioning of bots in the information system of organizations are analyzed.

The methods and means of detecting the functioning of bots in the organization's information system based on Splunk were studied. The purpose, main functions, composition and architecture of the Splunk solution are defined

On the basis of the research carried out in the work, a version of the technology for detecting the functioning of bots in the information system of the organization and recommendations for its application at the enterprise were developed.

The field of use is cyber security of the corporate information system.

INFORMATION SYSTEM, CYBER SECURITY, BOT, TECHNOLOGY OF BOT DETECTION IN THE INFORMATION SYSTEM

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ІС – інформаційна система;

ОС – операційна система;

ШПЗ – шкідливе програмне забезпечення;

С2 – командно-контрольний сервер;

CERT – computer emergency response team;

CSIRT – computer security incident response team;

IOC – indicator of compromise;

NBA – network behavioral analysis;

NGFW – next generation firewall;

SIEM – security information and event management;

SOC – security operation center;

TI – threat intelligence

ВСТУП

Актуальність дослідження. Шляхом підвищення ефективності бізнес-процесів сучасного підприємства є впровадження та застосування інформаційних технологій. З ростом інформаційних технологій, їх ускладненням та збільшенням різноманіття, зловмисники вигадували способи викрадення інформаційних, персональних та фінансових активів, залишаючи в компонентах інформаційних систем організації засоби для прихованого, віддаленого керування.

З моменту виникнення інформаційних технологій, виникла і бот-інфікування. Спеціалісти з кібербезпеки мусили постійно вигадувати нові способи захисту, виокремлювати використовувані зловмисниками злочинні патерни, та намагались завчасно передбачити дії зловмисників. З плином часу, світовий ринок пропозицій засобів забезпечення безпеки інформаційної системи організації переповнився. З ростом методів і засобів захисту від зловмисників з'явилась проблема децентралізації процесів кіберзахисту, у зв'язку з чим, з'явилась необхідність в централізованому місці для моніторингу стану захищеності ІС організації.

Вищенаведені аргументи актуалізують тему даної магістерської роботи, зміст якої становлять дослідження щодо технології виявлення функціонування ботів в інформаційних системах організації на базі Splunk.

Об'єкт дослідження – виявлення функціонування ботів в інформаційній системі організації.

Предмет дослідження – технологія виявлення функціонування ботів в інформаційній системі організації на базі Splunk.

Мета роботи – запропонувати технологію виявлення функціонування ботів в інформаційній системі організації та розробити рекомендацію щодо її застосування.

Наукові завдання:

дослідити сутність проблеми функціонування ботів в інформаційній системі організації;

встановити сутність завдань захисту інформаційних систем організації;

проаналізувати існуючі технології виявлення функціонування ботів в інформаційній системі організації;

проаналізувати методи та засоби забезпечення захисту від ботів інформаційних систем організації на базі Splunk;

проаналізувати основні функції та принципи реалізації захисту інформаційних систем.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання технології виявлення функціонування ботів в інформаційній системі організації.

Практичне значення одержаних результатів полягає в розробці варіанта технології виявлення функціонування ботів в інфомраційних системах організацій на базі Splunk та Splunk Enterprise Security, а також у розробці рекомендацій щодо застосування технології виявлення функціонування ботів в інформаційній системі орагнізації.

Апробація результатів магістерської роботи було оприлюднено на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2022 року в Державному університеті телекомунікацій, м. Київ.

1 АНАЛІЗ ПРОБЛЕМИ ВИЯВЛЕННЯ ФУНКЦІОНУВАННЯ БОТІВ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ

1.1 Аналіз проблеми виявлення функціонування ботів в інформаційній системі організації

Вся діяльність організації стосовно інформаційної системи зводиться до таких базових операцій: доходи, видатки, залишок, баланс, аналіз і планування [1]. Ці операції стосуються будь-яких об'єктів обліку, а саме: товари, матеріали, основні засоби, безготівкові і готівкові грошові кошти тощо. Практично всі бізнес-процеси підприємства чи будь-який вид економічної діяльності можна представити цими операціями (рис.1.1).

Рис. 1.1. Структурна схема інформаційної системи

ІС включає вхідну інформацію (дані, інструкції) та вихідну інформацію (звіти, розрахунки) і функціонує в інформаційному середовищі. За допомогою засобів обробки інформації вхідна інформація перетворюється на вихідну, і потім надсилається користувачу або іншій ІС. ІС може включати механізм зворотного зв'язку.

Термін “інформаційна система” належить до класу програмних продуктів, що автоматизують ведення бізнесу. Система називається інформаційною, якщо вона підтримує інформаційне забезпечення бізнесу.

Інформаційна система – це сукупність засобів збору, зберігання, передачі, оброблення інформації в певному апаратному, програмному, або апаратно-програмному середовищі для досягнення поставленої мети у процесі управління.

З вищевказаного визначення можна сформувати перелік функцій, котрі виконує ІС:

збирати інформацію;

зберігати інформацію;

передавати інформацію;

обробляти інформацію.

Методологічною основою функціонування ІС є системний підхід, відповідно до якого будь-яка система - це сукупність взаємопов'язаних об'єктів для досягнення загальної мети. Поведінка системи має ряд властивостей:

цілісність – поведінка окремих об'єктів розглядається з позиції структури всієї системи;

забезпечення стійкості функціонування системи;

адаптивність до змін зовнішнього середовища;

здатність до навчання шляхом зміни структури системи відповідно до зміни мети системи.

Умова виконання всіх вищепойменованих властивостей ІС є основним критерієм того, що вона функціонує правильно.

Характеристикою бот-інфікування є зараження шкідливим програмним забезпеченням, основною функцією якого є створення прихованого каналу зв’язку з сервером зловмисника, по котрому передаються та виконуються інфікованою машиною системні команди. Серверне обладнання, або робочі станції користувачів, котрі керуються за допомогою командного серверу зловмисника, називаються – *бот***.**

Ботнет — це мережа комп'ютерів, заражених зловмисним програмним забезпеченням, якими дистанційно керують зловмисники для отримання певної вигоди, задля вчинення деструктивних дій, порушення властивостей інформації котра або здійснення атак на об'єкти ІС. Коли комп'ютер інфікується ШПЗ, він встановлює з'єднання та отримує інструкції від командно-контрольних (C2) серверів, розташованих по всьому світу. Багато ботнетів призначені для збору даних, таких як паролі або логіни, номери соціального страхування, номери кредитних карток, адреси, номери телефонів та іншої особистої та корпоративної інформації. Використовуються ця інформація для цілей, таких як викрадення особистих даних, шахрайство з кредитними картками, спам або фішинг, атаки на веб-сайти та поширення шкідливого програмного забезпечення [2].

Проблема функціонування ботів та ботнетів з плином часу стає дедалі насущнішою. Згідно статистики 2021 року близько 40% світового інтернет трафіку становить бот трафік [3], а ретроспективний аналіз тенденції показував що вона зростала. З огляду на тенденцію, відсоток кількості бот трафіку, до загальної тільки ростиме.

Поодинокі хакери, їх спілки, а також організовані та спонсоровані державами хакерські угрупування демонструють досить високу гнучкість реалізації доставки ШПЗ до жертви. Але основним джерелом зараження ШПЗ на території України, згідно звіту Системи виявлення вразливостей та реагування на кіберінциденти та кібератаки за 3й квартал 2022 року є фішингові повідомлення [4]. Це підтверджує тезу про те, що найслабшою ланкою в системі кіберзахисту організації була та залишається людина.

Основним мотивом для створення ботів та ботнетів є гроші, адже це досить потужний ресурс для вчинення атак DDoS атак. Даний тип атаки слугує для підриву авторитетності, довіри до ресурсу.

7 серпня 2021 року хакерське угрупування ‘‘aihacker’’ зробило пост в мессенджері Telegram з розцінками на вчинення DDoS атаки потужностями на 1 Тбіт/сек UDP трафіку з метою вичерпання ресурсу пропускної здатності каналу зв’язку, або 140-500 Гбіт/сек ACK/SYN TCP трафіку з метою унеможливлення обробки такої кількості запитів серверами [2].

Приблизна оцінка грошового ресурсу, котрий надходить оператору ботнету, що включає в себе 5000-10000 ботів становить приблизно 10000 доларів на день [2].

1.2 Аналіз існуючих методів виявлення ботів та ботнетів в інформаційній системі організації

Для виявлення функціонування ботів та ботнетів в ІС організації, ця організація мусить мати персонал, котрий володіє відповідними компетенціями в галузі кібербезпеки, та відповідає за захист інформації, котра циркулює в ІС. Штат організації для виконання вищевказаних вимог може комплектуватись такими підрозілами, як:

SOC;

CERT;

CSIRT.

SOC (з англійської мови ‘‘Security Operation Centre”) – підрозділ котрий розробляє та імплементує політики безпеки, слідкує за їх дотриманням, збирає, зберігає та аналізує за допомогою SIEM системи журнали подій з усіх компонентів ІС таких як:

Серверне обладнання;

Користувацькі пристрої;

Мережеве обладнання;

Фаєрволи;

Системи виявлення/запобігання вторгненням;

Системи захисту кінцевих точок;

Інше обладнання.

CERT (з англійської мови ‘‘Computer Emergency Response Team’’) – команда реагування на кіберінциденти. Відповідає за усунення виявлених кіберінцидентів та унеможливлення їх повторення. Переважно функціонує разом з SOC командою, та кіберінцидентами, котрі вона виявляє.

CSIRT (з англійської мови ‘‘Computer Security Incident Response Team’’) – це команда виявлення та реагування на кіберінциденти. Складається зі спеціалістів інформаційної безпеки котрі слідкують за інфраструктурою ІС, аналізують журнали подій всіх компонентів ІС, виявляють кіберінциденти та усувають їх. Фактично це гібридна форма, котра включає в себе команди SOC та CERT.

Функціонування ботів в ІС організації завжди супроводжується певними хостовими, або мережевими паттернами, за допомогою яких і здійснюється виявлення бот-інфікування на різних стадіях вчинення реалізації кібератаки. Розділити кібератаку на стадії можна за допомогою логічної схеми Cyber Kill Chain [5] (рис.1.2.)

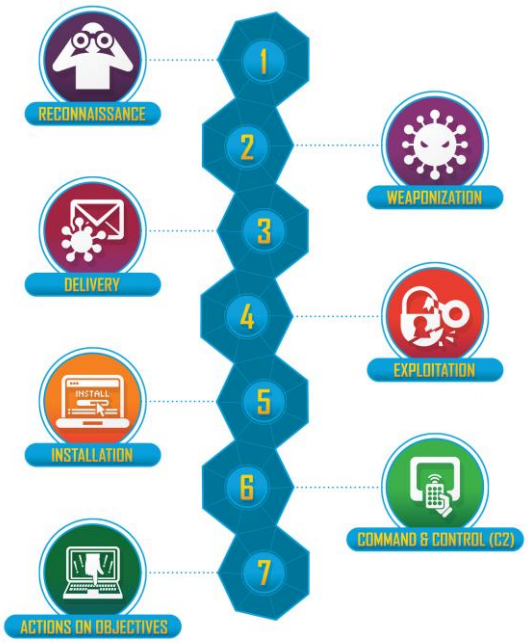

Рис. 1.2. Cyber Kill Chain

Reconnaissance (Розвідка) – зловмисникам здійснюється сканування компонентів ІС на предмет виявлення ‘‘точок проникнення’’ в організацію. Зазвичай використовують мережеві сканери, та сканери вразливостей з метою виявлення ресурсів, котрі не оновлювались, або мають місконфігурації котрі можна використати

Weaponization (Підготовка) – зловмисники виявивши ‘‘точку проникнення’’ готуються до здійснення кібератаки. На цьому етапі може здійснюватись збагачення інформації стосовно потенційної жертви з відкритих джерел, підкуп співробітників організації, створюється ШПЗ з метою експлуатації виявлених вразливостей, розробляється легенда для фішингових листів, налаштовується інфраструктура командного серверу і тд.

Delivery (Доставка) – з огляду на розроблену концепцію кібератаки на попередньому етапі зловмисники реалізують доставку ШПЗ в ІС організації.

Exploitation (Експлуатація) – в разі успішної доставки ШПЗ в ІС організації відбувається виконання зловмисного коду, експлуатація виявленої вразливості, чи місконфігурації або вчинення зловмисних дій підкупленим співробітником, залежно від обраної концепції кібератаки.

Installation (Закріплення) – етап, на котрому зловмисники вчиняють дії, спрямовані на унеможливлення втрати зв’язку з ботом. Типовим прикладом дії є створення задач в планувальниках задач операційних систем. Після закріплення в системі здійснюється заходи по втручанню в засоби безпеки ІС, або аналізуються безпекові політики та вчиняються дії по їх обходу, спрямовані для приховання слідів присутності боту, сприяння поширенню бот-інфекції по компонентам ІС, унеможливлення видалення ШПЗ, або вчинення інших зловмисних дій.

C2 (Встановлення з’єднання з сервером зловмисника) – після успішної стадії Експлуатації здійснюється реалізація прихованого каналу з’єднання до командно-контрольних серверів. Приховуватись канал може шляхом створення віртуальної приватної мережі, або маскування під легітимну активність, з метою

заплутання спеціалістів з інформаційної безпеки. Після успішного бот-інфікування, бот може отримати команди від зловмисника котрі послугують для інфікування інших компонентів ІС для реалізації ‘‘просування вшир’’ для створення ботнету та компрометації чутливої інформації.

Actions on objectives (Реалізація наміру) – на фінальному етапі зловмисник відправляє зібрані дані та/або виводить зі строю компоненти ІС під час свого знаходження в мережі жертв. Потім проводяться заходи для виявлення інших цілей, розширення своєї присутності всередині організації та вилучення даних.

Потім ланцюжок повторюється. Взагалі, особливостями Cyber-Kill Chain є те, що вона кругова, а не лінійна. Як тільки хакер проник в мережу, він знову починає цей ланцюжок всередині мережі, здійснює додаткову розвідку і виконує горизонтальне просування всередині вашої мережі.

Окрім того, необхідно враховувати, хоча методологія однакова, але при знаходженні всередині мережі зловмисники будуть використовувати для етапів внутрішнього ланцюжку засоби відмінні від тих, ніж у випадку, коли вони знаходяться поза мережею. Насправді, після проникнення хакера в мережу, він стає інсайдером (користувачем з визначеними правами та присутністю в мережі).

Класифікувати тактики та техніки, котрі використовують зловмисники можна за допомогою матриці MITRE ATTACK [6]. Дана матриця допомагає усвідомити можливі вектори кібератак, проаналізувати ІС на предмет виявлення потенційних ‘‘точок проникнення’’ при розробці політик безпеки і досить важливо слідкувати за повним покриттям даної матриці політиками.

Задача спеціалістів з інформаційної безпеки виявляти та присікати спроби бот-інфікування ІС організації на всіх етапах. В залежності від архітектури інформаційної безпеки в організації можна виокремити основні методи виявлення ботів на всіх етапах реалізації кібератаки. Потенційні патерни котрі послугують методами та засобами виявлення функціонування ботів в ІС організації наведені в таблиці 1.1.

Таблиця 1.1

Індикатори котрі використовуються в ході виявлення функціонування ботів в ІС організації

Етап	**Хостові**	**Мережеві**	**Засоби забезпечення інформаційної безпеки організації**
Розвідка	• Записи в журналах подій про відхилені з'єднання та нестандартні запити	• ICMP запити • Підвищення кількості спроб встановлення TCP сессій відносно нормалі • Велика кількість запитів від одного джерела за одиницю часу	Подія безпеки
Підготовка	Відсутні	Відсутні	Нестандартна поведінка персоналу
Доставка	• Вхідний електронний лист • Запит на завантаження файлу • Повідомлення про виконання макрос-запитів при відкритті файлу сімейства Microsoft Office • Нестандарна поведінка хосту (миготіння терміналу)	• Передача файлу	• Подія безпеки • Нестандартна поведінка персоналу

Продовження таблиці 1.1

Індикатори котрі використовуються в ході виявлення функціонування ботів в ІС організації

Етап	**Хостові**	**Мережеві**	**Засоби забезпечення інформаційної безпеки організації**
Експлуатація	• Нестандартна робота хосту (підвисання, незрозумілі артефакти)	• Підозрілий DNS-запит • Підозрілий HTTP(S) запит	Подія безпеки
Закріплення	• Несанкціоновані модифікації реєстру Windows • Несанкціоноване внесення змін до планувальника задач системи • Несанкціонована зміна конфігурацій сервісів	• Несанкціоновані внесення змін до конфігурацій обладнання	Подія безпеки
Встановлення з'єднання з сервером зловмисника	• Несанкціоноване TCP з'єднання	• Виникнення несанкціонованих VPN тунелів • Передача чутливої інформації в мережевій телеметрії	Подія безпеки
Реалізація наміру	• Нетипова поведінка системи	• Нетипова поведінка мережі	Подія безпеки

З огляду на наведену таблицю, найдієвішими методами виявлення функціонування ботів в ІС організації є імплементація в них системи та засобів забезпечення інформаційної безпеки, котрі будуть генерувати події безпеки, адмініструванням котрих буде займатись команда інформаційної безпеки.

1.3 Аналіз існуючих технологій виявлення функціонування ботів в інформаційній системі

Найдієвішим методом виявлення та протистояння функціонуванню ботів в ІС організації є імплементація в них засобів забезпечення інформаційної безпеки. Згідно еталонної моделі OSI ці засоби умовно можна розділити на 7 рівнів (рис.1.3) [7].

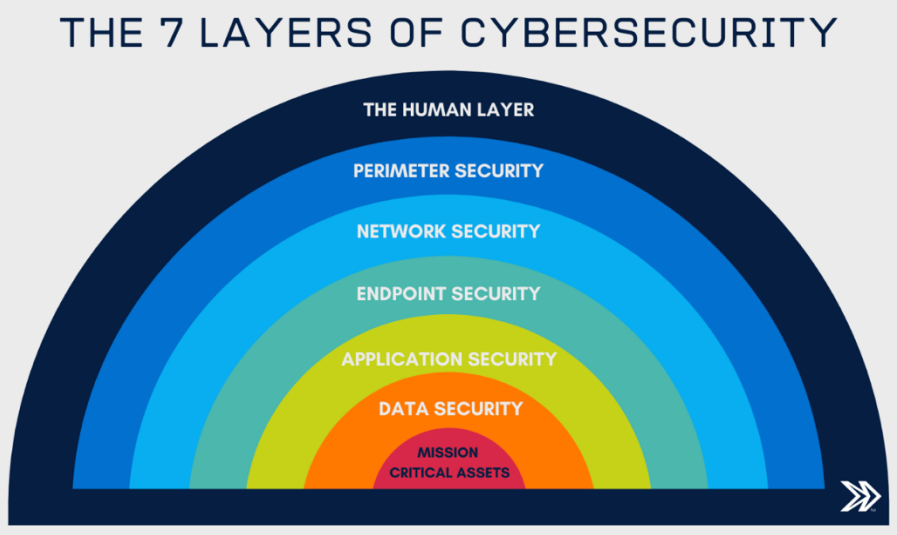

Рис. 1.3. Рівні забезпечення безпеки ІС

Mission critical assets (Визначення активів) – на цьому етапі організація має інвентаризувати всі свої активи, призначити їм пріоритетність, провести аналіз ризиків та розробити міри та плани котрі будуть прийматись в разі кіберінциденту.

Data security (Безпека даних) – міри котрі приймаються з метою забезпечення безпеки збереження інформаційних ресурсів, а також безпечного середовища їх передачі. Досягається шляхом використання правил безпечного налаштування середовища хостового та мережевого обладнання.

Application security (Безпека додатків) – конфігурація сервісів та служб, додатків при яких мінімізуються шанси експлуатації їх вразливостей.

Endpoint security (Безпека кінцевих точок) – створюється з метою систематичного аналізу файлів та процесів, котрі знаходяться/виконуються на

кінцевому обладнанні ІС організації для виявлення шкідливої активності, та присікання її.

Network security (Мережева безпека) – заходи, котрі приймаються з метою унеможливлення несанкціонованого доступу до мережі інформаційної системи.

Perimeter security (Створення контрольованої зони) – комплекс організаційно-технічних заходів, котрі розробляються та впроваджуються з метою усунення несанкціонованого доступу осіб до приміщень, обладнання та інших компонентів ІС з метою запобігання вчинення навмисних, або ненавмисних дій, котрі можуть спричинити пошкодження ІС або призвести до кіберінциденту.

The human layer (Робота з персоналом) – людина завжди була і буде найслабкішою ланкою в захищеній системі. Дани міри спрямовані на систематичне навчання всього персоналу ІС з кібергігієни, для того щоб зменшити ймовірність того що людина відкриє фішинговий лист, котрий пропустили засоби забезпечення безпеки пошти, наприклад.

Для забезпечення безпеки на всіх цих рівнях існують спеціальні технології, котрі можуть функціонувати як для зебезпечення одного з семи, так і для забезпечення декількох рівнів. Приклади технологій наведені в таблиці 1.2.

Таблиця 1.2

Технології котрі забезпечують захист ІС організації

Рівень безпеки	**Приклад технології котра забезпечує безпеку**
Визначення активів	SolarWinds Platform
Безпека даних	Tenable NC
Безпека додатків	Acunetix
Безпека кінцевих точок	Cisco AMP Endpoint
Мережева безпека	Cisco Firepower
Створення контрольованої зони	Hikvision Digital Technology
Робота з персоналом	Дія. Цифрова освіта

Вищезазначені технології задовольняють виконання лише одного з рівнів безпеки. Існують пропрієтарні технології компаній, котрі слугують для більшого

покриття рівнів загроз. Проте їх основним мінусом є досить важка імплементація в уже існуючі інфраструктури ІС, а інколи і неможлива, у зв'язку з особливостями архітектури, технічними вимогами до обладнання, використанням пропрієтарних протоколів обміну інформацією.

Ще однією важливою проблемою є відсутність централізованого місця, з централізованим менеджментом та загальною картиною стану захищеності ІС. Для вирішення цієї проблеми була розроблена технологія SIEM.

Характерною особливістю даної технології – є централізоване місце де збираються, зберігаються, обробляються журнали подій компонентів ІС, надходять та обробляються події безпеки. Дану технологію використовують SOC підрозділи. Вона гарно зарекомендувала себе і з року в рік показує досить високі результати росту попиту на ці технології, а компанії-розробники даних продуктів безперестанно займаються їх підтримкою, збільшенням можливостей з огляду на потреби фахівців, котрі їх використовують у своїй діяльності [8]. Приклади SIEM рішень наведені на матриці компанії Gartner 2022 року (рис. 1.4).

Рис. 1.4. Магічний квадрант Gartner

З огляду на наведену матрицю стає зрозуміло що різні компанії займають різні ніші та мають свої особливості, котрі задовольняють вимоги конкретної ІС.

Основними характеристиками технології SIEM – є комплексність бачення інформації та її аналізу, котру надсилають джерела даних ІС, а також їх можливості в виконанні аналітичних завдань спеціалістів команди інформаційної безпеки ІС.

Виходячи з вищенаведеної інформації та найкращих практик світових лідерів в галузі кібербезпеки доцільно задля забезпечення захисту ІС використовувати SOC підрозділ, котрий буде аналіхувати дані, агреговані технологією SIEM.

Задля коректної імплементації в ІС організації SOC підрозділу необхідно дотримуватись чітких стратегій функціонування підрозділу [9]:

Стратегія 1: знати, що захищається і чому. Розвивати ситуаційну обізнаність через розуміння місії; правове та технічне регулювання середовища даних, знати користувачів, їх поведінку і взаємодію з послугами, знати загрози. Надавати пріоритет інформації про критичні системи та дані, що в них циркулюють, періодично повторювати через деякий час.

Стратегія 2: надати SOC повноваження виконувати свою роботу. SOC повинен мати повноваження для виконання своїх функцій у сферах діяльності, партнерства та обов’язків. Досягається через затвердження правових норм, дотримання їх виконання і узгодження положень SOC всередині організації.

Стратегія 3: Створення структури SOC, яка б відповідала організаційним потребам, структурування SOC фахівців, відповідно до їх функцій та обов’язків.

Стратегія 4: Наймати та розвивати професійний персонал. Необхідно створити середовище, щоб залучати людей і заохочувати їх залишатися в організації, з наданням можливості прогресу кар’єрного та культурного. Перед створенням підрозділу необхідно продумати, скільки персоналу потрібно для різних SOC функції.

Стратегія 5: Пріоритезація реагування на інциденти. Підготуватися до обробки інцидентів, визначивши категорії інцидентів, кроки реагування та ескалацію, шляхи в розслідування кіберінцидентів та визначення відповідальних сторін (осіб). Також необхідно визначити пріоритети інцидентів для організації та розподілення ресурсів для реагування. Виконайти доповіді що функціональності бізнес-просесів, статусу захищенності ІС орагінзації з точністю і усвідомленням про місію та цілі.

Стратегія 6: Висвітлювати зловмисників за допомогою аналізу кіберзагроз. Адаптування збору і використання даних про кіберзагрози, аналізуючи інформацію про противника, становище організації та технічного середовища для визначення пріоритетів, захисту, моніторингу та інших дій.

Стратегія 7: Обрати і збирати дані правильно. Виберати дані, враховуючи відносну цінність різних типів даних, таких як дані датчиків і журналів ОС, зібрані мережевими та хост-системами, хмарними ресурсами, програмами та датчиками. В разі не слідування даній стратегії, через занадто малу кількість даних, може сформуватись відсутність актуального стану ІС організації, занадто багато даних, спровокують перевантаження аналітичних інструментів та персоналу.

Стратегія 8: Використання інструментів для підтримки робочого процесу аналітики. Відображення представлення в інструментах і даних, а також інтеграція їх, щоб максимізувати корисну дію робочих процесів SOC. Для досягнення підходять багато інструментів SOC, включаючи SIEM, UEBA, SOAR та інші, в усіх технічних компонентах організації, включаючи хмарні середовища.

Стратегія 9: Чітке спілкування, систематична співпраця. Взаємодія в рамках SOC, із зацікавленими сторонами та складовими, а також з ширшою кібернетичною спільнотою, щоб розвивати можливості та сприяти безпеці загалом.

Стратегія 10: Вимірювання ефективності для її покращення. Визначити якісні та кількісні показники, щоб знати, що працює добре і де необхідні

покращення. Показники SOC включає бізнес-цілі, джерела даних і збір, синтез даних, звітність, прийняття рішень і дії.

Стратегія 11: Збільшувати гнучність, розширивши функціональні можливості SOC. Покращити діяльність SOC, включивши відслідковування загроз, команди з тестування на проникнення, аналіз шкідливого програмного забезпечення, судово-медичні експертизи, навчання. Будь-який із наведених прикладів може покращити.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ ФУНКЦІОНУВАННЯ БОТІВ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ОРГАНІЗАЦІЇ НА БАЗІ SPLUNK

2.1 Призначення, можливості та функції Splunk

З огляду на наведену в попередньому розділі матрицю Gartner з порівняльною характеристикою SIEM систем, оптимальним рішенням котре буде задовольняти вимоги для забезпечення захисту ІС є SIEM Splunk. Адже він хоч і поступається в чомусь по функціоналу деяким іншим рішенням, проте має лідуючу позицію серед збалансованих показників комплекснісності бачення інформації та її аналізу, котру надсилають джерела даних ІС, а також їх можливості в виконанні аналітичних завдань спеціалістами команди інформаційної безпеки ІС.

Splunk забезпечує аналіз в реальному часі подій безпеки, отриманих від мережевих пристроїв і додатків. Даний продукт представлено додатками, приладами або послугами, і використовується також для журналювання даних і генерації звітів в цілях сумісності з іншими бізнес-даними.

Постачальники продають Splunk як програмне забезпечення, як прилади або як послуги. Також використовується для реєстрації даних безпеки та створення звітів.

Основними функціями Splunk є:

Агрегація даних: збирання журналів подій компонентів ІС. Дані збираються з різних джерел: мережеві пристрої та сервіси, датчики систем безпеки, сервери, бази даних, програми та інше. Забезпечується консолідація даних з метою пошуку критичних подій.

Кореляція: пошук спільних атрибутів, зв'язування подій у вагомі кластери. Технологія забезпечує застосування різних технічних заходів для інтеграції даних з різних джерел для перетворення вихідних даних в значущу інформацію.

Сповіщення: автоматизований аналіз корелюючих подій і генерація повідомлень (сигналів) про поточні проблеми. Оповіщення може виводитися на "приладову панель самого додатка, або бути направлено в інші сторонні канали: e-mail, месенджер, сайт, та інше.

Засоби відображення (інформаційні панелі): відображення діаграм, які допомагають ідентифікувати патерни відмінні від стандартної поведінки.

Сумісність (трансформування): застосування додатків для автоматизації збору даних, формування звітності для адаптації агрегованих даних до чинних процесів управління інформаційною безпекою та аудиту.

Зберігання даних: застосування довготривалого зберігання даних в хронологічному порядку для кореляції даних за часом та для забезпечення трансформування. Довготривале зберігання даних критично для проведення комп'ютерно-технічних експертиз, оскільки розслідування мережевого інциденту, зазвичай, відбувається з часовою затримкою від моменту порушення.

Експертний аналіз: можливість пошуку по безлічі журналів на різних вузлах.

Немалозначущою перевагою Splunk рішення є спільнота користувачів, в котрих є можливість ділитись своїми напрацюваннями на спеціальній платформі, впровадженій Splunk розробниками. Це можуть бути навчальні статті, написані висококваліфікованими спеціалістами з метою поділитись своїм досвідом зі всіма охочими, опубліковані на відповідному ресурсі. Публікації проходять редактуру Splunk команди з метою відсіяння неправдивої інформації. Також розробниками продукту був створений власний інтернет-магазин на котрому вони публікують або свої додатки, або дозволяються публікувати будь кому охочому. Додаток Splunk являє собою набір налаштувань, розроблених функцій, логіки, виконаний інструментами Splunk, доступними всім. Також присутні багато соціальних спільнот, в деяких з яких присутні навіть представники Splunk команди, що дає змогу всім охочим звернутись з питанням напряму до відповідальних за те, чи інше рішення людям.

Переважно обмін напрацюваннями відбувається на безоплатній основі з метою розвитку платформи та самопросування автора. Для прикладу взято додаток для Splunk, котрий автором розповсюджується безкоштовно [10]. Мета цього додатку – виявлення функціонування ботнетів в ІС організації. Основою діяльності цього додатку є штучний інтелект, котрим було проаналізована бот-телеметрія, а також трафік без нього.

Підхід, котрий був використаний - набір даних містить 20 мільйонів журналів NetFlow, які містять звичайний, фоновий і створений ботнетом трафік. Необроблені журнали NetFlow були зведені в 60-секундні вікна, де в кожному вікні обчислюється статистика для:

кількості потоків;

суми переданих байтів;

середня сума байт на NetFlow;

середній час зв'язку з кожною унікальною IP-адресою;

кількість унікальних IP-адрес призначення;

кількість унікальних портів призначення;

найбільш часто використовуваний протокол (наприклад, TCP, UDP).

Аналіз набору даних, намагаєтеся виявити, чи є зв’язок між характеристиками даних – статистичними даними, обчисленими для кожного 60-секундного вікна – та класом даних (ботнет чи не ботнет). Зокрема, на інформаційній панелі аналізу дослідницьких даних ви зможете побачити чітке розмежування між звичайним і ботнет-трафіком на панелі «Аналіз функцій за допомогою ботів» і «Звичайний трафік» (рис. 2.1).

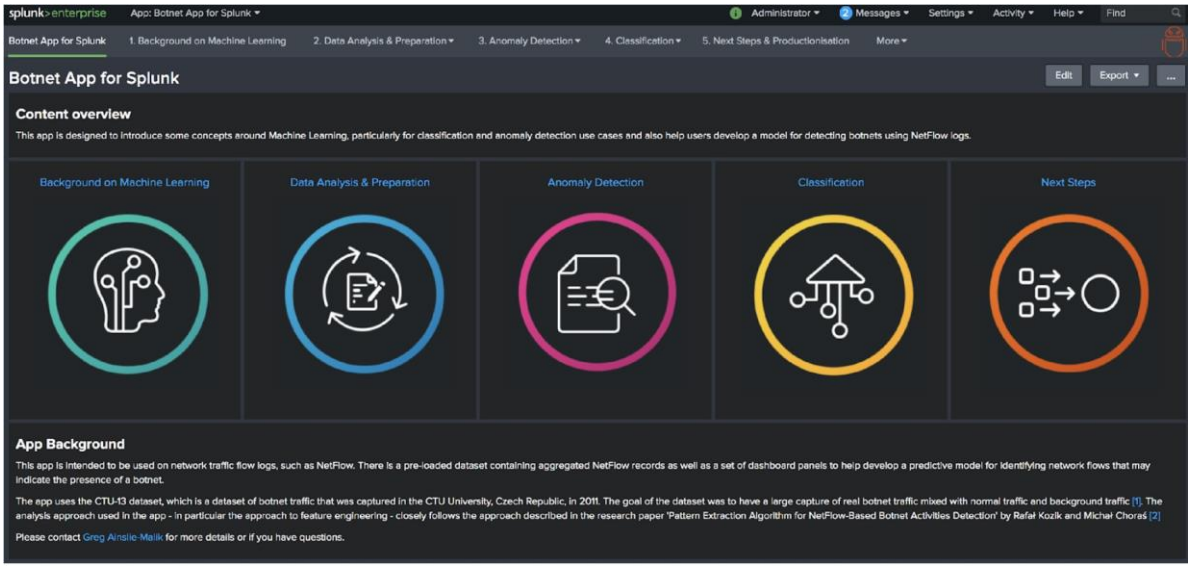

Рис.2.1. Інформаційна панель Botnet App for Splunk

Працює алгоритм в 3 етапи:

1. Аналіз та попередня обробка даних;
2. Виявлення аномалії;
3. Класифікація.

SIEM Splunk широковживаний спеціалістами з кібербезпеки та має досить великий спектр застосування. Незалежність від пропрієтарних рішень, невибагливість в джерелах даних, гнучкий функціонал з налаштування обробки та зберігання даних, величина спілки та безкоштовні результати її діяльності – усе це робить Splunk гарним рішенням для імплементації в ІС організації з метою виявлення функціонування ботів.

2.2 архітектура та компоненти рішення Splunk

Splunk – це розподілена система, яка приймає, обробляє та індексує дані журналу. Splunk обробляє дані в три етапи:

1. Введення даних – Splunk отримує потік необроблених даних із джерела, розбиває його на блоки по 64 КБ і додає ключі метаданих, зокрема ім’я хоста, джерело, кодування символів та індекс, у якому дані мають зберігатися.

2. Зберігання даних – Splunk аналізує дані журналів подій, розбиваючи їх на рядки, ідентифікуючи мітки часу, створюючи окремі події та анотуючи їх ключами метаданих. Потім він перетворює дані події за допомогою правил перетворення, визначених оператором. Зрештою, Splunk записує проаналізовані події на диск, вказуючи на них із файлу індексу, що забезпечує швидкий пошук у великих обсягах даних.

3. Пошук даних – на цьому етапі Splunk дозволяє користувачам запитувати, переглядати та використовувати дані подій. Виходячи з потреб користувача у звітності, він створює такі об’єкти, як звіти, інформаційні панелі та сповіщення.

Splunk доступний у трьох версіях:

Splunk Light – безкоштовна версія;

Splunk Enterprise – платна версія;

Splunk Cloud – надається як послуга з ціною передплати.

Відмінності між версіми наведені в таблиці таблиці 2.1.

Таблиця 2.1

Відмінності між версіями Splunk

Версія Splunk	**Обмеження**	**Архітектурні можливості**
Splunk Light	Індексація до 500 Мб на день	Не підтримує розподілену архітектуру
Splunk Enterprise	Необмежений	Підтримує кластеризацію на одному датацентрі та кластеризацію на кількох датацентрах для аварійного відновлення
Splunk Cloud	Залежно від пакету послуг	Кластеризація під керуванням команди Splunk

Основними компонентами в архітектурі Splunk є форвардер, індексер і пошуковик [11] (рис. 2.2).

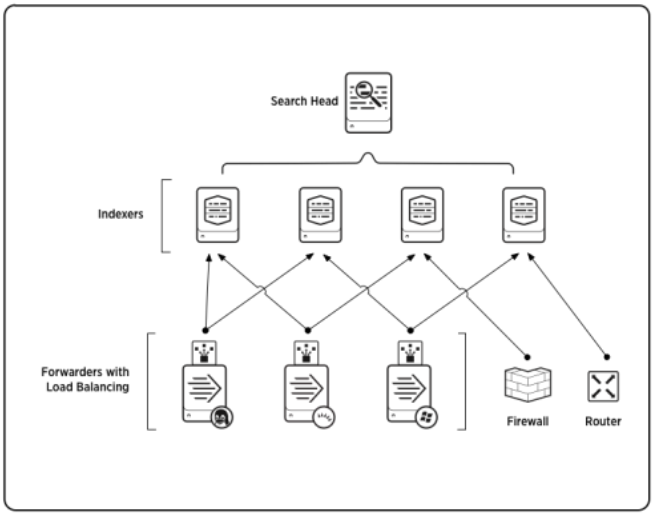

Рис. 2.2. Компоненти Splunk

Форвардер (Forwarder) – це агент, встановлений в ІС на хості, який збирає журнали операційної системи та надсилає їх до індексера. Splunk має два типи форвардерів:

Універсальний форвардер (Universal forwarder) – пересилає необроблені дані без попередньої обробки. Це швидше та потребує менше ресурсів на хості, але призводить до надсилання величезної кількості даних до індексера.

Важкий форвардер (Heavy forvarder) – виконує синтаксичний аналіз та індексування в джерелі, на головній машині, і надсилає лише проаналізовані події до індексера.

Індексер (Indexer) перетворює дані в події (якщо вони не були отримані попередньо обробленими від важкого форвардеру), зберігає їх на диску та додає до індексу, що забезпечує можливість пошуку. Індексер створює такі файли, розділяючи їх на каталоги, які називаються сегментами:

Стиснуті вихідні дані

Індекси, що вказують на необроблені дані (файли .TSIDX)

Файли метаданих

Індексер виконує загальну обробку подій журналів операційних систем та інших лог-файлів, наприклад, застосовує позначку часу та додає джерело, а також

може виконувати визначені користувачем дії перетворення, щоб отримати певну інформацію або застосувати спеціальні правила, наприклад фільтрацію небажаних подій.

Також існує можливість для налаштування кластеру з індексерів із реплікацією даних між ними, щоб уникнути втрати даних і надати більше системних ресурсів і місця для зберігання та обробки великих обсягів даних.

Пошуковик (Search head) надає інтерфейс користувача, який спеціалісти можуть використовувати для взаємодії з Splunk. Він дозволяє користувачам шукати та запитувати дані Splunk, а також взаємодіє з індексерами, щоб отримати доступ до конкретних даних, які вони запитують.

Splunk дає можливість створити архітектуру розподіленого пошуку, яка дозволяє масштабувати роботу з великими обсягами даних, а також краще контролювати доступ і географічно розподілені дані. У сценарії розподіленого пошуку керівник пошуку надсилає пошукові запити групі індексерів, які також називаються одноранговими пошуковими вузлами. Індексери виконують пошук локально та повертають результати пошуковику, яка об’єднує результати та повертає їх користувачеві.

Наступна діаграма детально ілюструє архітектуру Splunk (рис. 2.3).

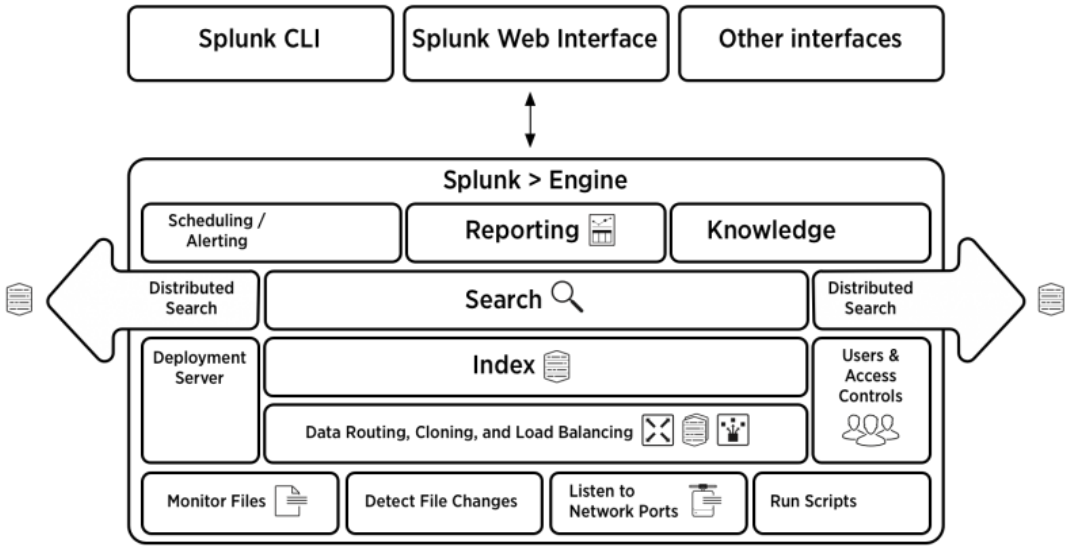

Рис. 2.3. Детальна архітектура Splunk

Splunk збирає дані, відстежуючи файли, виявляючи зміни файлів, прослуховуючи порти або запускаючи сценарії для збору даних журналу – усе це виконує програма пересилання Splunk.

Механізм індексації, що складається з одного або кількох індексерів, обробляє дані або може отримувати дані, попередньо оброблені форвардерами.

Сервер управління керує індексерами та заголовками пошуку, конфігурацією та політиками в усій інфраструктурі Splunk.

Доступ і засоби керування користувачами застосовуються на рівні індексера – кожен індексер можна використовувати для іншого сховища даних, яке може мати різні дозволи користувача.

Пошуковик використовується для забезпечення функціональності пошуку за вимогою, а також забезпечує пошук за розкладом, ініційований автоматичними звітами.

Користувач може визначити об’єкти Scheduling, Reporting і Knowledge для планування пошуку та створення сповіщень.

Доступ до даних можна отримати через веб-інтерфейс користувача, Splunk CLI або API, інтегровані з численними зовнішніми системами.

Широка архітектурна гнучкість, можливість масштабування, невибагливість до першоджерела збирання інформація, повністю закритий цикл обробки інформації з можливостями індивідуальних налаштувань – атрибутує Splunk як доцільну технологію для виявлення функціонування ботів в інформаційній системі організації.

2.3 Призначення та архітектура рішення Splunk Enterprise Security

Splunk Enterprise Security (ES) вирішує широкий спектр аналітики безпеки ІС та випадків використання операцій, включаючи безперервний моніторинг безпеки, розширене виявлення загроз, відповідність, розслідування інцидентів, криміналістику та реагування на кіберінциденти. Splunk ES надає наскрізне

уявлення про стан безпеки організацій із гнучкими дослідженнями, неперевершеною продуктивністю та найбільш гнучкими варіантами розгортання, які пропонуються в хмарних, локальних або гібридних моделях розгортання. Splunk ES основні переваги на відміну від Splunk Enterprise:

Налаштувати точкове сповіщення про події безпеки з імплементацією пріоритизації їх за допомогою високоточного оповіщення на основі ризиків;

Забезпечення видимості у гібридному середовищі за допомогою багаторівневого моніторингу безпеки;

Гнучкі дослідження для ефективного виявлення загроз у джерелах безпеки, та кінцевих пристроях;

Модуль для інвентаризації та пріоритизації інформаційних активів Asset Manager;

Інтегрована бібліотека з готовими сценаріями безпекової кореляції інформації в разі відсутності інших компонентів забезпечення інформаційної безпеки ІС;

Велика кількість графіків, котрі відображають стан захищеності ІС з відображення покриття площини атак на ІС за допомогою використання матриці MITTRE;

Велика кількість додатків, котра спрощує нормалізацію даних (їх приведення до загального вигляду), зменшуючи кількість роботи для спеціалістів з інформаційної безпеки.

Splunk ES надає дуже зручний функціонал для опрацювання подій безпеки, з можливістю налаштування безпекових кореляцій, дуже гнучкими налаштуваннями фільтрації подій безпеки завдяки багатьом міткам та тегам котрі додаються до подій безпеки (рис.2.4). Також представлені модулі для моніторингу покриття площини загроз, реєстрування та проведення кіберінцидентів, моніторингу «видимості» інформаційних активів, модуль Threat Intellidgence моніторингу та кореляцій, функціонал, котрий дозволяє привести всі джерела даних до загального вигляду та значно пришвидшити відпрацювання пошуків

Пошуковиком шляхом наповнення та акселерації датамоделей, та дуже велика бібліотека завчасно налаштованих безпекових кореляційних правил.

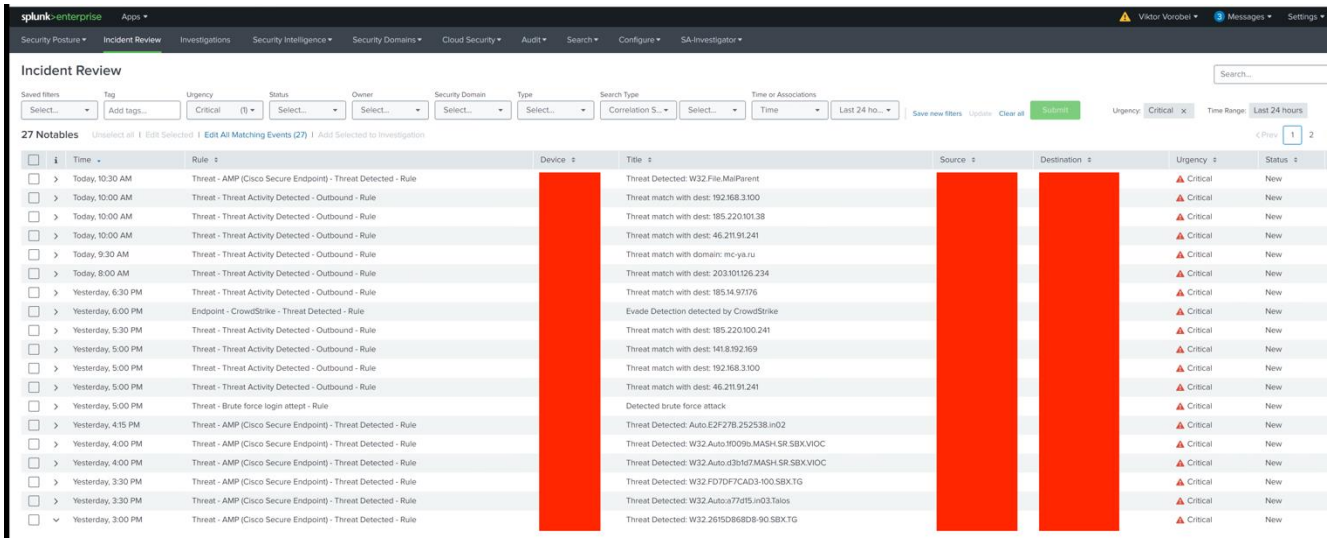

Рис.2.4. Інформаційна панель з відображенням подій безпеки Splunk ES

Інформаційні панелі (Dashboards) – це відображення статистичної інформації, які складаються з панелей. Панелі можуть містити такі модулі, як вікна пошуку, поля, діаграми, таблиці та списки. Панелі приладів зазвичай підключаються до звітів [12].

Створивши пошукову візуалізацію або зберігши звіт, можна додати її до нової або наявної інформаційної панелі. Існує також редактор інформаційних панелей, за допомогою якого можна створювати та редагувати інформаційні панелі. Редактор інформаційної панелі корисний, якщо є набір збережених звітів, які потрібно швидко додати на інформаційну панель (рис.2.5).

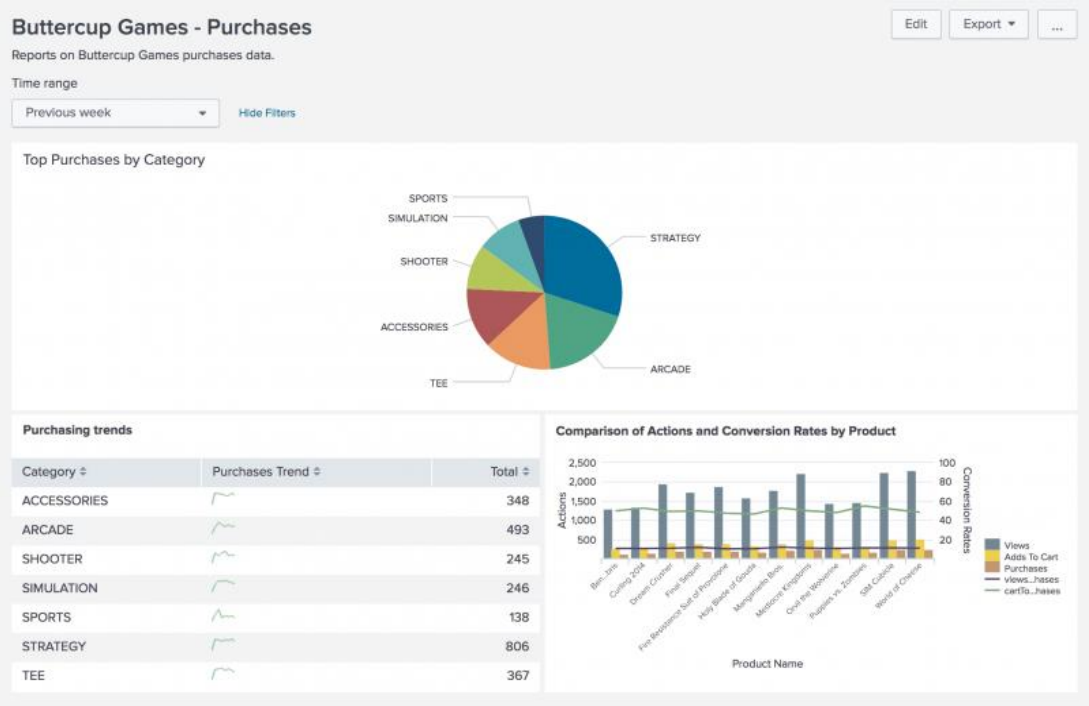

Рис.2.5. Приклад інформаційної панелі

Інформаційні панелі дозволяють відслідковувати відхилення від нормалі, відображати сповіщення – результати роботи пошуків, структурузовувати великі обсяги інформації і надавати її в лаконічному, графічному форматі.

Немалозначущою перевагою рішення Splunk Dashboards є те, що спеціалісти з досить великою технічною базою можуть репрезентувати результати своєї діяльності в довільному форматі, котрий буде зрозумілий менш кваліфікованим, або навіть зовсім некваліфікованим особам. Цей функціонал досить часто використовується SOC-as-a-service командами, де команда репрезентує результати своєї роботи клієнтам без обізнаності в сфері кібербезпеки.

3 ВАРІАНТ ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ФУНКЦІОНУВАНННЯ БОТІВ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ НА БАЗІ SPLUNK

3.1 Розроблення варіанта технології виявлення функціонування ботів в інформаційній системі організації на базі Splunk

На базі Splunk виявляти функціонування ботів в ІС організації можна за допомогою аналізу:

1. Мережевої телеметрії;
2. Хостових ідентифікаторів;
3. Правил кореляції 1-го та 2-го пункта за допомогою кореляційних правил;

В ході розробки варіанта технології були враховані всі вказані методи виявлення функціонування ботів в інформаційній системі. Проте як згадувалось раніше, найефективніше застосовувати їх комплексно з метою виявлення бота на кожному з етапів Cyber Kill Chain щоб покрити всю площину загроз ІС.

В демонстраційних цілях була розроблена тестова лабораторія для перевірки працездатності технології. Тестова лабораторія виступає в ролі інформаційної системи в котрій циркулюють інформаційні дані, компоненти котрої піддаються атакам типу бот.

Для демонстрації виявлення ботів в ІС за допомогою наведених вище методів використовувалась тестова лабораторія, зображена на рисунку 3.1

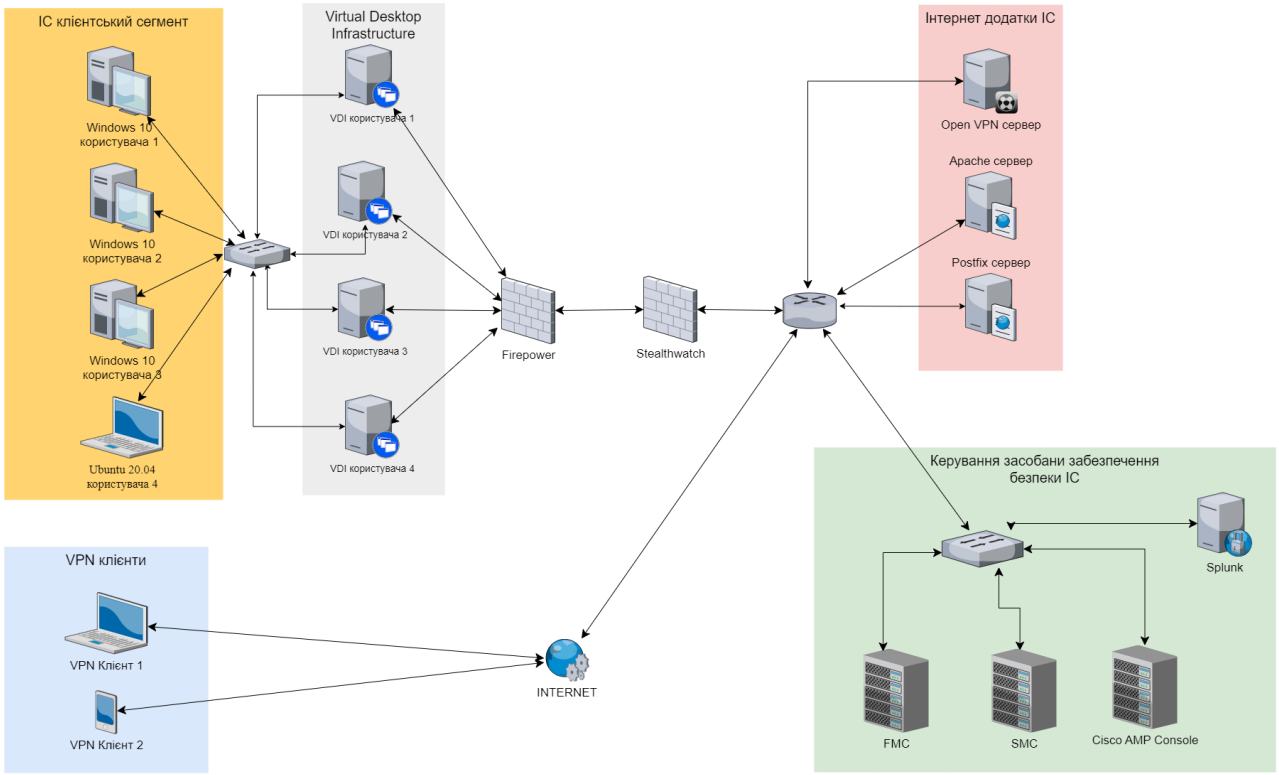

Рис.3.1. Логічна схема тестового стенду

Інформаційна система наведена на схемі поділена на сегменти:

Клієнтський сегмент – цей сегмент IC складається з робочих станцій користувачів організації, що являють собою персональні комп'ютери та ноутбуки, які слугують користувачам як засіб під'єднання до віртуального робочого місця.

Virtual Desktop Infrastructure (Віртуальні робочі місця) – безпосередньо віртуальні машини користувачів з котрих відбувається адміністрування IC, тобто робочі машини напряму не мають доступу до інфраструктури інформаційної системи. Використовується в робочих місцях операційна система Windows 10. Побудований сегмент віртуальних робочих місць за допомогою VmWare Horizon.

VPN сегмент – в організації розгорнуто Open VPN Server задля надання спеціалістам можливості віддаленого доступу до організації з використанням двофакторної Google автентифікації. На персональних робочих станціях спеціалістів з інформаційної безпеки встановлений OpenVPN клієнт, котрий під'єднується до сервера створюючи шифрований тунель.

Інтернет додатки ІС – інформаційна система має свої інтернет додатки доступ до котрих надається всім користувачам Інтернету, у зв'язку з чим, ці додатки систематично піддаються веб-атакам зловмисників. Даний сегмент містить поштовий сервер Postfix та веб-сервер Apache на котрому розміщений корпоративний сайт організації.

Засоби забезпечення безпеки ІС – в інформаційній системі використовується NGFW (Next-Generation Firewall – виконує функції фаєрвола на всіх рівнях еталонної моделі OSI, а також здійснює сигнатурний аналіз мережевого трафіку) *Firepower* та NBA (Network Behavior Analysis – здійснює аналіз сессій, та поведінковий аналіз мережевого трафіку, у своєму складі має штучний інтелект, котрий відповідає за виявлення аномалій) *Stealthwatch*. Також використовується рішення *Cisco Security Endpoint* для захисту кінцевих точок. На кожному кінцевому пристрої встановлено агент, котрий здійснює моніторинг операційної системи та керується за допомогою Cisco AMP Console.

Firepower Management Console (FMC) – консоль для централізованого управління NGFW Firepower.

StealthWatch Management Console (SMC) – консоль для централізованого управління NBA StealthWatch.

Всі засоби забезпечення безпеки ІС надсилають події безпеки в SIEM Splunk. Додатково збираються та аналізуються всі журнали подій із всіх компонентів ІС. Firepower передає дані на Splunk за допомогою пропрієтарного протоколу передачі (та формату) даних *eStreamer*. Stealtwatch надсилає події безпеки за допомогою протоколу *Syslog* (також протокол передачі і відображення даних, але не пропрієтарний компанії Cisco, а загальнодоступний). Консоль AMP надсилає данні в форматі *JSON*. На решті обладнання встановлені універсальні форвардери, котрі пересилають журнали подій операційних систем Windows та Linux Ubuntu. На серверному обладнанні ІС, яке знаходиться в сегменті Інтернет додатків, окрім журналів подій збираються і журнали застосунків, котрі встановлені на серверах.

Функціонування ботів залишає ознаки присутності в ІС, записи в журналах подій, котрі відслідковуються за допомогою правил безпекової кореляції компонентів забезпечення безпеки ІС (Firepower, Stealthwatch, AMP for Endpoints, Splunk).

Splunk ES надає дуже зручний функціонал для опрацювання подій безпеки, з можливістю налаштування безпекових кореляцій, дуже гнучкими налаштуваннями фільтрації подій безпеки завдяки багатьом міткам та тегам котрі додаються до подій безпеки. Також представлені модулі для моніторингу покриття площини загроз, реєстрування та проведення кіберінцидентів, моніторингу «видимості» інформаційних активів, модуль Threat Intellidgence моніторингу та кореляцій, функціонал, котрий дозволяє привести всі джерела даних до загального вигляду та значно пришвидшити відпрацювання пошуків Пошуковиком шляхом наповнення та акселерації датамоделей, та дуже велика бібліотека завчасно налаштованих безпекових кореляційних правил.

3.1.1 Розроблення варіанта технології виявлення функціонування ботів в інформаційній системі організації на базі Splunk при аналізі мережевої телеметрії

При аналізі мережевої телеметрії можна виявити «маячки» котрі в телеметрії передає бот для встановлення з’єднання з командно-контрольним сервером зловмисника. Виявити бота при аналізі мережевої телеметрії можна за допомогою наступних методів:

Маячки відомих зразків ШПЗ;

DGA;

Кореляція з ТІ-платформами .

Для зразку взято ШПЗ типу Cobalt Strike, котре загальновживане зловмисниками та добре відоме спеціалістам з інформаційної безпеки.

Cobalt Strike – це комерційне програмне забезпечення для симуляції

противника, яке продається пентест командам, але також викрадається та активно використовується широким колом загрозливих суб'єктів, від операторів програм-вимагачів до APT угрупувань, орієнтованих на шпигунство [13]. Для належного функціонування даного ШПЗ має бути налаштований командно-контрольний сервер, та бот, котрий керується сервером. Характерною особливістю використання даного ШПЗ є комунікація між ботом та C2 сервером за допомогою 50050/TCP порту. Створивши кореляційне правило можна відслідковувати подібну активність в ІС організації та легко виявляти функціонування ШПЗ Cobalt Strike (рис.3.2)

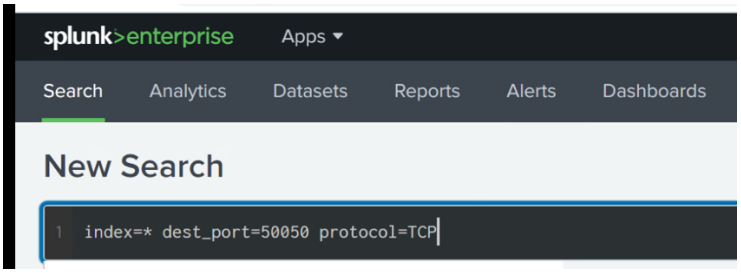

Рис.3.2. Кореляційне правило для виявлення маячків відомих ШПЗ

DGA (Domain Generation Algorithms) – дана техніка використовується зловмисниками в розробці ШПЗ задля приховування слідів комунікації бота з C2 сервером. Даний алгоритм створений для рандомізації доменних імен, котрі реєструються на короткі терміни, та слугують для приховування реальної IP-адреси зловмисника. Це математичний алгоритм, котрий є частиною ШПЗ. В момент запуску, запускається і математичний алгоритм, котрий прораховує певну послідовність опираючись на незалежні параметри (наприклад час в якійсь країні), на основі цього параметру створюється псевдорандомізована послідовність, котра слугує під-доменом. Завдяки незалежному параметру відбувається синхронізація ботів та C2 серверів, у зв'язку з чим інфіковані боти завжди отримають актуальну адресу C2 серверу, без втручання в цей механізм

людини, а ШПЗ може масово розповсюджуватись без якоїсь цілі, створюючи ботнет шляхом неконкретизованого розповсюдження.

Приклад DGA запиту виявленого за допомогою логування DNS трафіку наведено на рисунку 3.3.

Рис. 3.3. DGA запит

Splunk дозволяє створювати TI-колекції, котрі корелюються з мережевим трафіком і в разі співпадіння створюють подію безпеки. Дані колекції зберігаються в лукап-таблицях, наповнення котрих може відбуватись мануально, або автоматично з певним оновленням задля підтримання TI-коллекції в актуальному стані (рис.3.4)

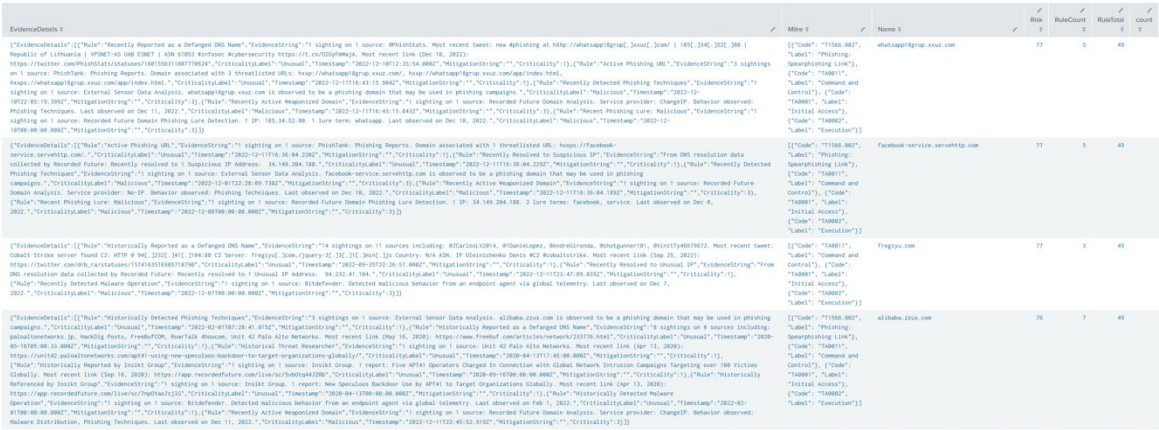

Рис.3.4 Приклад лукап-таблиці з наповненою інформацію стосовно фішингових деменних імен

Дані таблиці корелюються з мережевим трафіком за допомогою SPL правила зображеного на рисунку 3.5.

Рис.3.5. Кореляційне правило для TI кореляцій

3.1.2 Розроблення варіанта технології виявлення функціонування ботів в інформаційній системі організації на базі Splunk при аналізі хостових ідентифікаторів

Для комплексного захисту в ІС організації мають бути впроваджені засоби захисту кінцевих точок. При інфікуванні кінцевої точки буде вчинено ряд заходів, котрі допоможуть відслідкувати активність та заблокувати її.

Засіб забезпечення захисту кінцевих точок Cisco AMP проаналізував завантажений файл на хост та зробив висновок, що цей файл є шкідливим та згенерував подію безпеки (рис. 3.6). Проте в ІС організації досить часто є бізнес процеси, котрі не можна переривати. Дані системи можуть спрацювати хибно виставивши легітимну активність за шкідливу, заблокувавши її, тим самим перервавши процес. Досить актуальним це питання є в підрозділах по розробленню програмного забезпечення, адже недопрацьований продукт може бути прийнятий за потенційно шкідливий, та видалений засобом захисту.

Задля запобігання подібної активності та підтримання цілісності бізнес-процесів, в деяких випадках, рішення про блокування чи видалення приймає людина в ході аналізу події безпеки. Враховуючи, що підсистема захисту кінцевих точок ІС є лише однією зі складових компонентів кіберзахисту ІС, події безпеки, котрі вона генерує були направлені для аналізу в SIEM Splunk, задля

повідомлення аналітиків інформаційної безпеки про подію та прийняття остаточного рішення.

З огляду на подію безпеки зображену на рисунку 3.6 проаналізований файл позиціонується як шкідливий. Проте аналітик інформаційної безпеки проаналізувавши подію, переглянувши перелік легітимного ПЗ, котре встановлене на хості прийшов до виснувку що це легітимна програма, розроблена підрозділом організації для ведення бухгалтерського обліку. Видаливши це програмне забезпечення порушились би бізнес-процеси підрозділу діловодства організації.

Рис. 3.6. Подія безпеки Cisco AMP

Завдяки інтегруванню в систему забезпечення кібербезпеки ІС Splunk рішення зменшуються ризики допущення хибних спрацювань та порушенню бізнес-процесів під час виявленні зловмисних ШПЗ на кінцевих точках організації.

В разі відсутності в організаціїї засобів забезпечення захисту кінцевих точок за допомогою SIEM Splunk можна виявляти функціонування ботів шляхом аналізу

журналів подій операційних систем. Перелік подій ОС Windows, котрі варто логувати та аналізувати наведено в таблиці 3.1 [14].

Таблиця 3.1

Перелік хостових індикаторів ОС Windows, котрі необхідно відслідковувати задля виявлення функціонування ботів в ІС організації.

Код події	**Опис**	**Навіщо збирати?**
1102	Журнал аудиту очищено	Звичайна стратегія для зловмисників, які потрапляють у середовище, — прибрати сліди.
1104	Журнал безпеки заповнено	Подія вказує на те, що журнали безпеки заповнюються заповнено і треба приймати міри.
1108	Помилка служби реєстрації подій	Слугує для відслідковування що події безпеки збираються неперервно.
4624	В обліковий запис успішно ввійшли	Подія інформує про успішний вхід в систему, необхідно для відслідковування авторизації нелегітимних аккаунтів.
4625	Не вдалося ввійти в обліковий запис	Ця подія безпеки, яку необхідно відстежувати, дозволяє виявляти всі види потенційно зловмисної поведінки, оскільки атаки грубої сили є одними з найпоширеніших.

Продовження таблиці 3.1

Перелік хостових індикаторів ОС Windows, котрі необхідно відслідковувати задля виявлення функціонування ботів в ІС організації.

Код події	**Опис**	**Навіщо збирати?**
4672	Спеціальні привілеї, призначені новому входу	Назва цієї події дещо збиває з пантелику – вона не вказує на те, що користувачеві було надано спеціальні привілеї, більше того, що обліковий запис, який має спеціальні привілеї, увійшов у систему – тому ви побачите це разом із подіями 4624. Це слід контролювати, щоб виявити шахрайські облікові записи суперкористувачів або облікові записи з надмірними привілейованими правами.
4698	Створено заплановане завдання	Зловмисники та шкідливі програми часто створюють заплановані завдання, щоб забезпечити їх стійкість у середовищі. Відстежуючи цю подію разом із подією 4700, можна спостерігати за створенням підозрілих або невідомих запланованих завдань.
4700	Заплановані завдання ввімкнено	Див. 4698

Продовження таблиці 3.1

Перелік хостових індикаторів ОС Windows, котрі необхідно відслідковувати задля виявлення функціонування ботів в ІС організації.

Код події	**Опис**	**Навіщо збирати?**
4720	Обліковий запис користувача створено	Це скоріше код події для відстеження середовища, однак зловмисники іноді створюють для них облікові записи, які можуть використовувати та керувати ними, якщо вони отримали певний доступ. Їх слід відстежувати як для виявлення цієї активності, так і для того, щоб просто побачити, що відбувається у ІС.
4723	Була зроблена спроба змінити пароль облікового запису	Виявляє, що користувач намагається змінити свій власний пароль, а не пароль іншого облікового запису. У більшості випадків ви побачите це, коли користувач не може змінити свій пароль через те, що новий пароль не відповідає політиці паролів.
4725	Обліковий запис користувача вимкнено	Код події перевірки середовища, оскільки зловмисники зазвичай не прагнуть зробити вимкнення облікового запису. Однак це може допомогти виявити аномальну активність, яку слід дослідити.
4727	Групу створено (глобально)	Це, а також інші створення груп, слід відстежувати здебільшого для перевірки середовища, однак зловмисники іноді створюють групи.
4728	Користувача додано до глобальної групи	Див. 4727

Продовження таблиці 3.1

Перелік хостових індикаторів ОС Windows, котрі необхідно відслідковувати задля виявлення функціонування ботів в ІС організації.

Код події	**Опис**	**Навіщо збирати?**
4731	Групу створено (локально)	Див. 4727
4732	Користувача додано до локальної групи	Див. 4727
4740	Обліковий запис заблоковано	Код події для моніторингу привілейованих облікових записів, оскільки він дає хороший показник того, що хтось може намагатися отримати до нього доступ. Цей код також може вказувати, коли є неправильно налаштований пароль, який може блокувати обліковий запис.
4754	Групу створено (універсальну)	Див. 4727
4756	Користувача додано до універсальної групи	Див. 4727
4767	Обліковий запис користувача розблоковано	Див. 4727
4768	Запитано квиток автентифікації Kerberos	Коди подій автентифікації Kerberos слід відстежувати так само, як події автентифікації 4625 і 4624. Ці коди подій Kerberos, як правило, нададуть чіткіше уявлення про весь процес спроби входу, включно з тим, на якому етапі процесу не вдалося ввійти – попередня автентифікація чи публікація.
4771	Помилка попередньої автентифікації Kerberos	Цей код події слід реєструвати та обробляти так само, як події 4625. Windows має різні правила щодо того, коли реєструється 4625 і 4771, і це представляє набагато більш глибоке обговорення автентифікації. Для наших цілей знайте, що 4771 будуть гучними (думайте про кешовані паролі), але їх можна уточнити, вимкнувши поле коду результату.

Продовження таблиці 3.1

Перелік хостових індикаторів ОС Windows, котрі необхідно відслідковувати задля виявлення функціонування ботів в ІС організації.

Код події	**Опис**	**Навіщо збирати?**
4776	Контролер домену спробував перевірити облікові дані для облікового запису	Ця подія запускатиметься з робочих станцій і серверів так само, як і з контролера домену. Це також код події, який буде, якщо щось автентифіковано за допомогою NTLM, а не Kerberos, тому його також важливо включити в журнал автентифікації
4780	ACL було встановлено для облікових записів, які є членами груп адміністраторів	Перевірка середовища та ризик безпеки в рівних частинах, слугує для виявлення причин, чому ACL було змінено для цих облікових записів, і переконання, що це було легітимно.
4782	Здійснено доступ до хешу пароля облікового запису	Доступ до хешу має бути запланований, а незапланований доступ до хешу може становити загрозу безпеці або зловмисну діяльність
4798	Було перераховано членство користувача в локальній групі	Для цього та 4799, що перевіряється, може бути ознакою підозрілої поведінки, оскільки багато зловмисників, отримавши доступ до облікового запису, намагатимуться перевірити, наскільки цінним є їхній обліковий запис, до якого вони отримали доступ.
4799	Було перераховано членство в локальній групі з підтримкою безпеки	Див. 4798

Системний монітор (Sysmon) – це системна служба Windows та драйвер пристрою, який після встановлення в системі залишається резидентом під час перезавантаження системи, щоб відстежувати та реєструвати системні дії в журналі подій Windows. Він надає докладні відомості про створення процесів, мережеві підключення та зміни часів створення файлів. Збираючи події, створені за допомогою колекції подій Windows або агентів Splunk, а потім аналізуючи їх, можна визначити шкідливі або аномальні дії та зрозуміти, як зловмисники та шкідливі програми працюють в мережі [15].

Sysmon включає такі можливості:

Записує до журналу створення процесу за допомогою повного командного рядка як для поточного, так і для батьківського процесів.

Записує хеш файлів процесів за допомогою SHA1 (за замовчуванням), MD5, SHA256 або IMPHASH.

Включає процес GUID у подіях створення процесу, щоб забезпечити кореляцію подій, навіть якщо Windows повторно використовує ідентифікатори процесів.

Реєструє завантаження драйверів або бібліотек DLL зі своїми сигнатурами та хешами.

Журнали відкриваються для необробленого доступу для читання дисків і томів.

У разі потреби реєструє мережеві підключення, включаючи вихідний процес кожного підключення, IP-адреси, номери портів, імена вузлів та імена портів.

Виявляє зміни у часі створення файлу, щоб зрозуміти, коли файл був створений. Змінення позначок часу створення файлів – це метод, який зазвичай використовується шкідливими програмами для.

Автоматичне перезавантаження конфігурації при зміні реєстру.

Фільтрування правил динамічного включення або виключення певних подій.

Створює події на ранніх етапах завантаження для відстеження дій, що виконуються шкідливими програмами в режимі ядра.

Кореляція подій за допомогою SIEM Splunk надає можливості проводити гібридний аналіз хостових та мережевих ідентифікаторів, що в свою чергу, дозволяє підтвердити, або спростувати теорію, розроблену в ході виявлення функціонування боту в ІС організації. Даний підхід дає більш комплексне бачення ситуації, алгоритмів дій зловмисника, виокремлення патерну, ідентифікування всіх бот-інфікованих хостів та збагачує доказову базу для підтвердження

кіберінциденту.

3.2 Варіант технологія виявлення ботів за допомогою Splunk Enterprise Security

Splunk Enterprise Security фреймворк дозволяє корелювати всі події безпеки з джерел забезпечення кібербезпеки ІС, а також інших компонентів ІС організації. Даний фреймворк надає можливості з:

Security Posture – надає функціонал для слідкування за SOC-метриками, аналізу площини загроз, функціональної здатності кореляційних правил, в ході аналізу яких здійснювати покращення в бізнес-процесах з виявлення функціонування ботів, та вдосконалення кореляційних правил.

Incident Review – централізоване місце для зберігання та обробки подій безпеки з усіх компонентів ІС організації.

Investigation – надає можливості в проведенні розслідуванні кіберінцидентів, виявлені всіх артефактів, зберігання та управління ними.

Security Intelligence – приймає участь в розслідуванні площини загроз інфраструктури.

Security Domains – навігація по галузям безпеки ІС організації.

Audit – надає можливості для інвентаризації своїх інформаційних активів, налаштувань над ними, та перевірки коректності роботи кожного з цих компонентів окремо та в цілому.

Search – виконує функції пошуковика.

Configure – надає можливості з конфігурування безпекових кореляцій, управління інформаційними активами, генеруванням подій безпеки, TI-кореляції.

При правильно нормалізованих даних, аналітики інформаційної безпеки будуть звертатись не напряму до надісланої інформації, котра зберігається в індексах, а до їх нормалізованої (приведеної до загального вигляду), сумморалізованої (проведені завчасно певні статистичні обчислення) та

акселерованої (агрегованої таким чином, що доступ і опрацювання здійснюються швидше) форми. Подібну форму даних надають датамоделі (рис.3.7). Саме цей функціонал дозволяє агрегувати і стандартизувати всі джерела даних до стандартного вигляду. Наприклад поля з різних джерел даних, котрі несуть одну й ту саму логічну суть будуть називатись однаково, що полегшує роботу спеціалістам інформаційної безпеки.

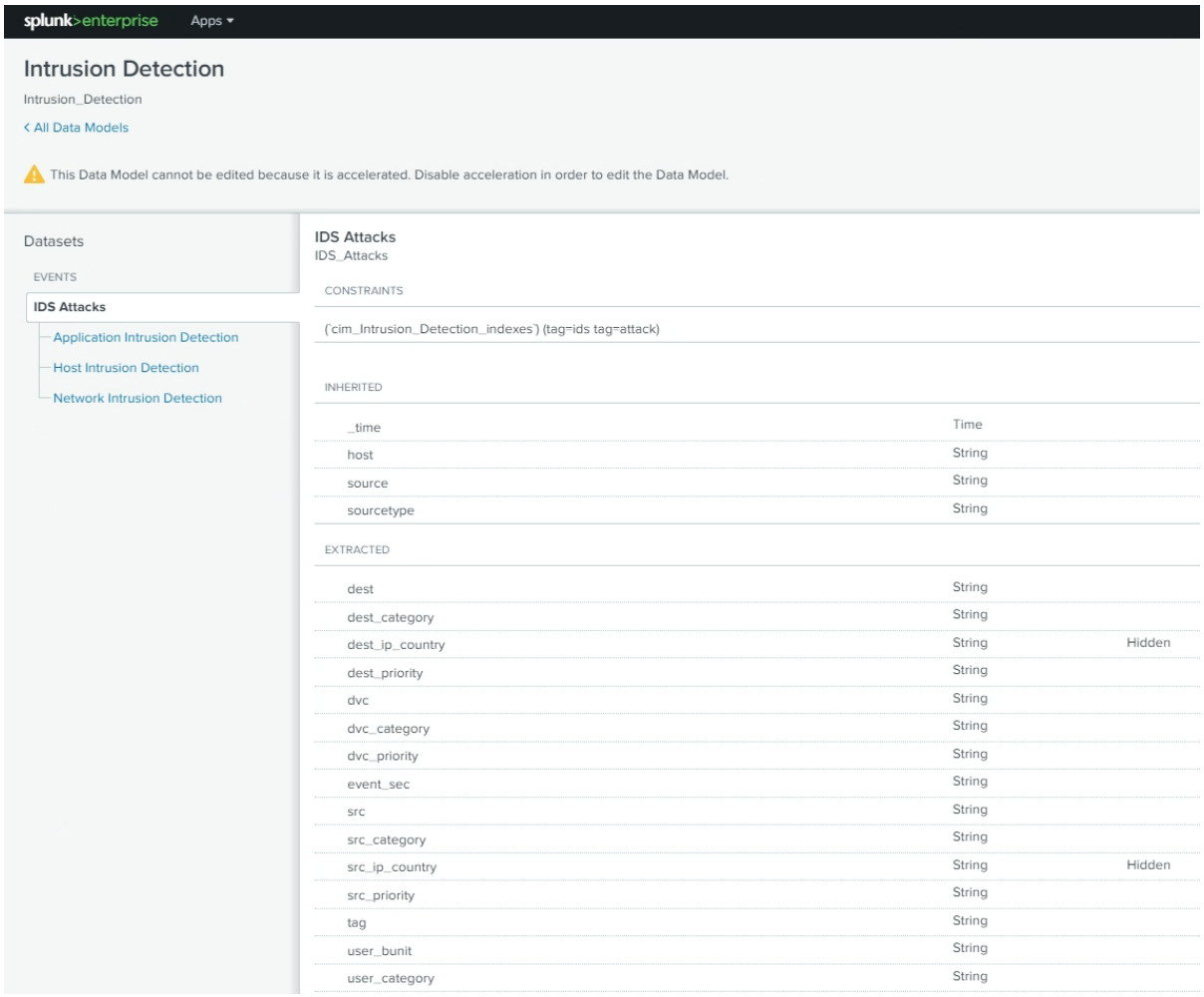

Рис. 3.7. Налаштування полів датамоделі

В тестовій лабораторії встановлено NGFW Firepower з сигнатурним, та NBA Stealthwatch з поведінковим аналізом трафіку з метою виявлення функціонування ботів. Дані засоби забезпечення захисту ІС мають відмінну один від одного структуру лог-файлу (Firepower для логування використовує пропрієтарний формат Estreamer, Stealthwatch - Sysmon), але незважаючи на це, доступ формат

представлення даних, завдяки правильній нормалізації, уніфікований. Доступ до даних датамоделі здійснюється за допомогою SPL запитів і відображається в статистичному форматі (рис.3.8).

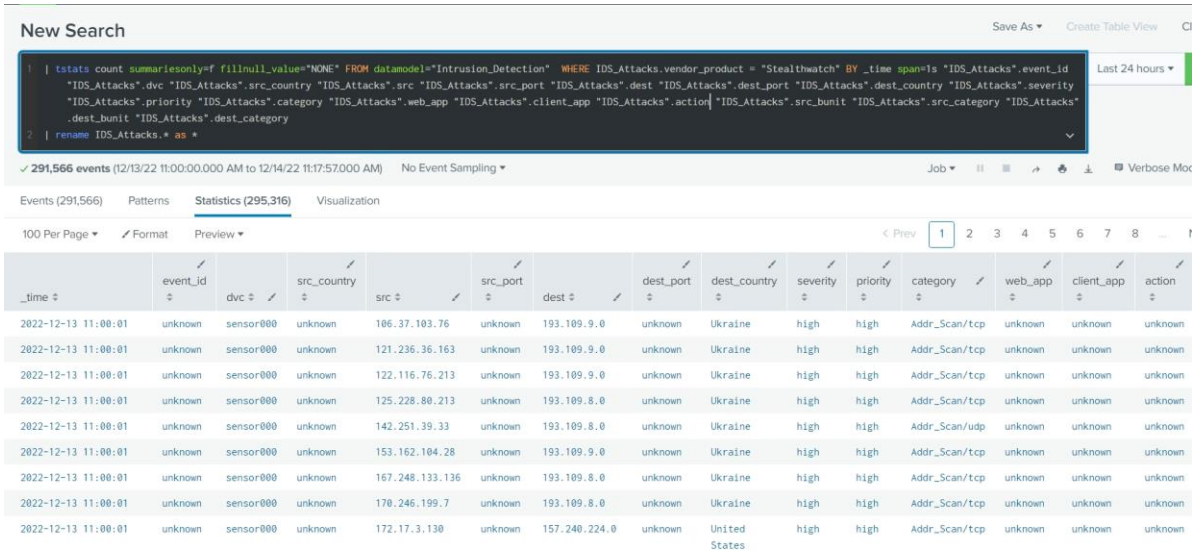

Рис. 3.8. Виявлення функціонування ботів, котрі здійснюють сканування ІС організації за допомогою датамоделі

Модуль Incident Review фреймворку Enterprise Security відіграє ключову роль в ознайомленні спеціалістами з інформаційної бепеки з подіями безпеки ІС, їх аналізі, ескалації кіберінциденту в разі необхідності. Даний модуль надає всю необхідну інформацію для проведення розслідування (Рис.3.9).

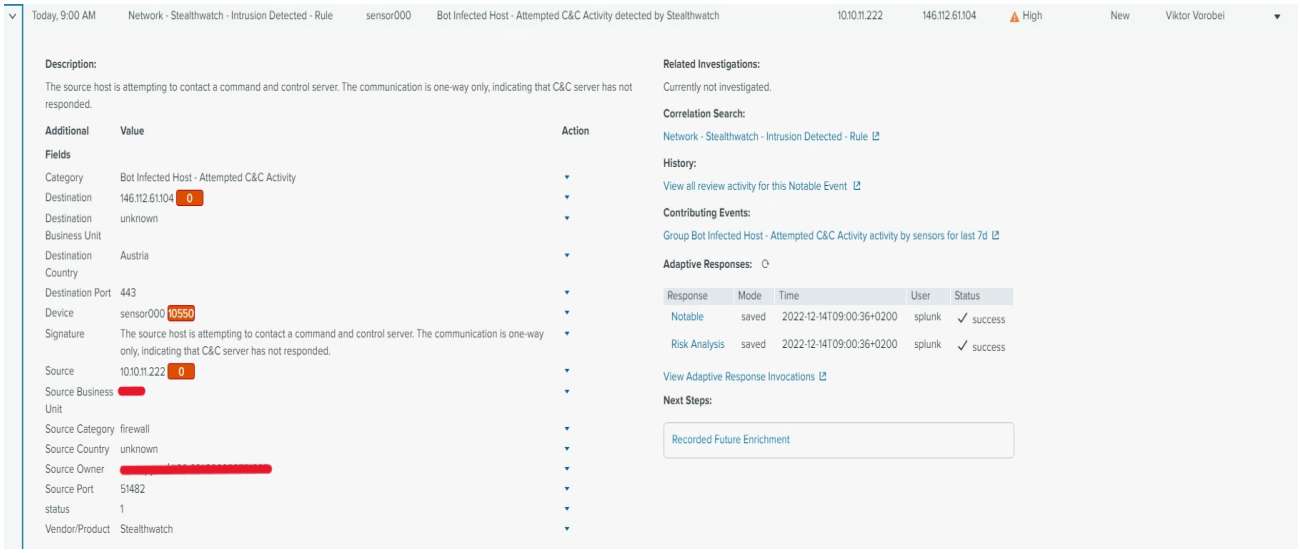

Рис 3.9. Відображення події безпеки Splunk Enterprise Security

Технологія Splunk Enterprise Security є безкомпромісним рішенням для виявлення функціонування ботів в ІС організації, завдяки колекціонуванню і упорядкованості інформації зі всіх систем, можливостям створювати безпекові кореляції і централізованого управління інформаційними активами.

3.3 Розроблення рекомендацій щодо застосування технології виявлення функціонування ботів в інформаційній системі організації

Виявлення функціонування ботів в інформаційній системі організації досить загальна і комплексна сутність, котру можна реалізовувати по різному і це не буде помилкою. Запропонована технологія на базі Splunk дозволяє реалізовувати абсолютно всі методи захисту ІС від ботів на всіх етапах Cyber Kill Chain, з метою повного покриття площини загроз і унеможливлення здійснення кіберінциденту ІС організації.

Часто під час функціонування ботів здійснюється типова активність, котра створює дуже багато типових подій безпеки, що в свою чергу ‘‘засмічує’’ місце їх відображення і відволікає спеціалістів з інформаційної бепеки від дійсно шкідливої активності. Типовою ситуацію може бути активність під час ведення зловмисниками розвідки, а саме – активне сканування. Зловмисники надсилають запити на TCP/UDP порти одного хосту, в Splunk може бути налаштоване правило на створення події безпеки в разі якщо відбувається спроба підключення на недобревідомі порти через що буде створено багато тисяч подій безпеки. Під час продумування безпекових кореляцій цей факт треба враховувати. В цьому випадку з’являється необхідність в налаштуваннях event suppressing (декілька пов’язаних подій безпеки об’єднуються в одну). Може бути налаштовано на фільтрацію по одному, або декільком полям котрі містяться в події бепеки. В разі правильних налаштувань, у випадку, наприклад сканування буде всього лише одна подія безпеки, котра буде оброблятись згідно аналітичного процесу.

Необхідно налаштовувати постійний моніторинг доступності коспонентів інформаційної системи. Потенційно може статися ситуація, коли у зв’язку з відсутністю даних, спеціалістом з інформаційної безпеки може бути прийнята ситуація за відсутність спроб атак.

При застосуванні даної технології, для її належного функціонування, спеціалісти мають володіти високим рівнем компетенції.

+ пару сторінок

ВИСНОВКИ

Інформаційна система - це сукупність засобів збору, зберігання, передачі, оброблення інформації в певному апаратному, програмному, або апаратно-програмному середовищі для досягнення поставленої мети у процесі управління.

Основним мотивом для створення ботів та ботнетів є гроші, адже це досить потужний ресурс для вчинення атак DDoS атак. Даний тип атаки слугує для підриву авторитетності, довіри до ресурсу.

Найдієвішими методами виявлення функціонування ботів в ІС організації є імплементація в них системи та засобів забезпечення інформаційної безпеки, котрі будуть генерувати події безпеки, адмініструванням котрих буде займатись команда інформаційної безпеки.

Основними характеристиками технології SIEM – є комплексність бачення інформації та її аналізу, котру надсилають джерела даних ІС, а також їх можливості в виконанні аналітичних завдань спеціалістів команди інформаційної безпеки ІС.

Виходячи з вищенаведеної інформації та найкращих практик світових лідерів в галузі кібербезпеки доцільно задля забезпечення захисту ІС використовувати SIEM технологію.

SIEM Splunk широковживаний спеціалістами з кібербезпеки та має досить великий спектр застосування. Незалежність від пропрієтарних рішень, невибагливість в джерелах даних, гнучкий функціонал з налаштування обробки та зберігання даних, величина спілки та безкоштовні результати її діяльності – усе це робить Splunk гарним рішенням для імплементації в ІС організації з метою виявлення функціонування ботів.

Кореляція подій за допомогою SIEM Splunk надає можливості проводити гібридний аналіз хостових та мережевих ідентифікаторів, що в свою чергу,

дозволяє підтвердити, або спростувати теорію, розроблену в ході виявлення функціонування боту в ІС організації. Даний підхід дає більш комплексне бачення ситуації, алгоритмів дій зловмисника, виокремлення патерну, ідентифікування всіх бот-інфікованих хостів та збагачує доказову базу для підтвердження кіберінциденту.

Splunk ES надає дуже зручний функціонал для опрацювання подій безпеки, з можливістю налаштування безпекових кореляцій, дуже гнучкими налаштуваннями фільтрації подій безпеки завдяки багатьом міткам та тегам котрі додаються до подій безпеки (рис.2.3). Також представлені модулі для моніторингу покриття площини загроз, реєстрування та проведення кіберінцидентів, моніторингу «видимості» інформаційних активів, модуль Threat Intellidgence моніторингу та кореляцій, функціонал, котрий дозволяє привести всі джерела даних до загального вигляду та значно пришвидшити відпрацювання пошуків Пошуковиком шляхом наповнення та акселерації датамоделей, та дуже велика бібліотека завчасно налаштованих безпекових кореляційних правил.

Технологія Splunk Enterprise Security є безкомпромісним рішенням для виявлення функціонування ботів в ІС організації, завдяки колекціонуванню і упорядкованості інформації зі всіх систем, можливостям створювати безпекові кореляції і централізованого управління інформаційними активами.

ПЕРЕЛІК ПОСИЛАНЬ

1. Інформаційна система [Електронний ресурс] – Режим доступу: https://pidru4niki.com/1222090547713/informatika/informatsiyni_sistemi

2. THE BUSINESS OF FRAUD:Botnet Malware Dissemination [Електронний ресурс] – Режим доступу: https://pub-7cb8ac806c1b4c4383e585c474a24719.r2.dev/b46634e31db6e507d518b51c52bcb70d6d4e8787.pdf

3. Barracuda Research Reveals Skyrocketing Levels Of Bot Traffic [Електронний ресурс] – Режим доступу:https://www.prnewswire.com/news-releases/barracuda-research-reveals-skyrocketing-levels-of-bot-traffic-301366777.html

4. Перший щорічний звіт функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки Державної служби спеціального зв'язку та захисту інформації України [Електронний ресурс] – Режим доступу: https://scpc.gov.ua/article/123

5. Cyber Kill Chain [Електронний ресурс] – Режим доступу: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

6. Mitre matrix [Електронний ресурс] – Режим доступу: https://attack.mitre.org/

7. The 7 levels of OSI model [Електронний ресурс] –Режим доступу: https://www.mvps.net/docs/the-7-layers-of-the-osi-model/?gclid=Cj0KCQiAtICdBhCLARIsALUBFcGtDuyJRFHVS-sYSALXrRPWOipTT63GOjv-mXI5zOxslj8CoR3FyEAaApRdEALw_wcB

8. Security information and event management (SIEM) Reviews and Rating [Електронний ресурс] – Режим доступу: https://www.gartner.com/reviews/market/security-information-event-management.

9. 11 Strategies of a World-Class Sybersecurity Operations Center [Електронний ресурс] – Режим доступу:

https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf

10. Botnet App for Splunk [Електронний ресурс] – Режим доступу: https://splunkbase.splunk.com/app/4816?_ga=2.2414963.25722876.1670729207-205072499.1655127081.

11. Splunk Architecture [Електронний ресурс] – Режим доступу: https://cloudian.com/guides/splunk-big-data/splunk-architecture-data-flow-components-and-topologies/#:~:text=Splunk%20provides%20a%20distributed%20search,indexers%2C%20also%20called%20search%20peers.

12. About Dashboards [Електронний ресурс] – Режим доступу: https://docs.splunk.com/Documentation/Splunk/9.0.2/SearchTutorial/Aboutdashboards

13. Defining Cobalt Strike components [Електронний ресурс] – Режим доступу: https://www.mandiant.com/resources/blog/defining-cobalt-strike-components

14. Windows event logs – what shoud monitor? [Електронний ресурс] – Режим доступу: https://www.criticalstart.com/windows-security-event-logs-what-to-monitor/

15. Sysmon version 14.12 [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/ru-ru/sysinternals/downloads/sysmon

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (ПРЕЗЕНТАЦІ)