Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
завідувач кафедри кібербезпеки
та захисту інформації
_____ Н.В. Лукова-Чуйко
« » червня 2021р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

дипломної роботи
бакалавра
(назва освітнього рівня)

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітня програма Кібербезпека
(назва освітньої програми)

на тему: «Методи та засоби захисту від APT атак»

Виконавець: студентка IV курсу, групи КБ-42

_____ **Мостовенко Анна Віталіївна**
(підпис) (прізвище ім'я по-батькові)

	Прізвище, ініціали	**Підпис**
Керівник	Зюбіна Р. В.	

Нормоконтроль	Зюбіна Р. В.	

Київ 2021

Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри кібербезпеки
та захисту інформації
_____Н.В. Лукова-Чуйко
«10» жовтня 2020 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студентці **КБ-42** (група) **Мостовенко Анні Віталіївні** (прізвище ім'я по-батькові)

Тема дипломної роботи Методи та засоби захисту від APT атак

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №2 від 08.10.2020 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Модель розгортання APT атаки, принципи розгортання SOC та його компонентів

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно ознайомитися з теорією розгортання APT атаки, методами захисту від неї, ознайомитися з принципами розгортання SOC та його основних компонентів, розробити графічне представлення роботи SOC в інфраструктурі та рекомендації для користувачів та адміністраторів, а також дослідити можливості SIEM системи.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розроблені рекомендації можна використовувати для навчання співробітників, а графічне представлення використовувати на початковому етапі впровадження SOCв інфраструктуру підприємства.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання:12 жовтня 2020 року

Завдання видала _____ Р. В. Зюбіна
(підпис) (ініціали, прізвище)

Завдання прийняла до виконання _____ А. В. Мостовенко
(підпис) (ініціали, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	25.01.2021 – 27.01.2021	*виконано*
2	Аналіз літератури	28.01.2021 – 11.02.2021	*виконано*
3	Обґрунтування вибору рішення	12.02.2021 – 14.02.2021	*виконано*
4	Дослідження APT атак	15.02.2021 – 28.02.2021	*виконано*
5	Дослідження характеристик SOC та його основних компонентів	01.03.2021 – 21.03.2021	*виконано*
6	Вироблення рекомендацій для користувачів та адміністраторів і розробка графічного представлення роботи SOC	22.03.2020 – 11.04.2020	*виконано*
7	Дослідження можливостей SIEM системи	12.04.2021 – 02.05.2021	*виконано*
8	Оформлення пояснювальної записки	03.05.2021 – 08.06.2021	*виконано*
9	Підготовка до захисту дипломної роботи	09.06.2021 – 21.06.2021	*виконано*

Завдання видала _____ Р. В. Зюбіна
(підпис) (ініціали, прізвище)

Завдання прийняла до виконання _____ А. В. Мостовенко
(підпис) (ініціали, прізвище)

Термін подання дипломної роботи до ЕК 08 червня 2021 року

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків, має 77 сторінок основного тексту, 5 таблиць та 31 рисунок. Список використаних джерел містить 25 найменувань і займає 3 сторінки.

Метою даної роботи є детальне вивчення принципів розгортання APT атаки, SOC та його компонентів.

У роботі проаналізована існуюча література з розгортання, виконання, аналізу APT атак, а також принципів розгортання, впровадження та подальшого функціонування SOC та його основних компонентів SIEM, NTA та EDR систем.

Розроблені рекомендації призначені для адміністраторів та користувачів, що мають на меті покращити рівень безпеки інформаційних систем та підвищити рівень обізнаності, а також зменшити ризики стороннього проникнення.

Розроблене графічне представлення роботи SOC в інфраструктурі підприємства слугує основним початковим етапом при впроваджені SOC в інфраструктуру підприємства і відображає основні зв'язки між його компонентами – SIEM, NTA та EDR.

Досліджено можливості роботи SIEM системи Splunk та розроблено власні графіки вибірок.

Ключові слова: APT атака, модель Kill Chain, зловмисники, SOC, SIEM, NTA, EDR.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

API	–	Application Programming Interface
APT	–	Advanced persistent threat
CVE	–	Common Vulnerabilities and Exposures
DNS	–	Domain Name System
DMZ	–	Demilitarized Zone
EDR	–	Endpoint Detection and Response
FTP	–	File Transfer Protocol
HTTP	–	HyperText Transfer Protocol
HTTPS	–	HyperText Transfer Protocol Secure
IaAM	–	Identity and access management
IDS	–	Intrusion Detection System
IP	–	Internet Protocol
IPS	–	Intrusion Prevention system
NTA	–	Network traffic analysis
OSINT	–	Open Source Intelligence
SIEM	–	Security information and event management
SOC	–	Security Operations Center
SSH	–	Secure Shell
SSL	–	Secure Sockets Layer
TCP	–	Transport Layer Security
USB	–	Universal Serial Bus
VOIP	–	Voice over IP
VPN	–	Virtual Private Network
ІБ	–	Інформаційна безпека
СУБД	–	Система управління базами даних

ЗМІСТ

ВСТУП

Актуальність даної роботи визначається тією обставиною, що APT атаки на критично важливі підприємства державної інфраструктури все частіше реалізуються з метою інформаційної боротьби з державами-опонентами.

10 травня 2021 року відбулася кібератака на трубопровід Colonial Pipeline в США, після чого міністерство транспорту США ввели надзвичайний стан в декількох штатах, а ціни на нафто продукти почали підвищуватися. Дана атака є яскравим прикладом поєднання державних та економічних інтересів хакерів. Підвищення рівня безпеки є важливим не тільки для державних компаній, але й для приватних.

Аналіз останніх досліджень та літератури. Вчені, які зробили вклад у вивчення APT атак: Ping Chen, Faisal Ali Garba, Венеамин Левцов, Николай Демидов та інші.

Метою роботи є аналіз принципів розгортання APT атаки, SOC та його компонентів, а також розробка рекомендацій щодо налаштування механізмів безпеки в інфраструктурі підприємства.

Для досягнення поставленої мети необхідно вирішити такі *завдання*:

- провести опитування задля виявлення прогалин у навчанні співробітників;
- розробити методичні вказівки для навчання співробітників підприємства;
- розробити графічне представлення роботи SOC в інфраструктурі підприємства;
- розробити рекомендацій щодо налаштування безпекових механізмів в інфраструктурі підприємства.

Об'єктом дослідження в даній роботі є процес розгортання APT атаки та способів захисту від неї.

Предметом дослідження в даній роботі є методи, засоби і рекомендацій щодо експлуатації безпекових механізмів в інфраструктурі підприємства.

Методи дослідження у дипломній роботі:

- аналіз літератури;
- аналіз документів;
- проведення опитування;
- вивчення та узагальнення вітчизняної і зарубіжної практики.

РОЗДІЛ 1
АРТ АТАКА

1.1 Характеристика APT атаки

Існує величезна кількість різних видів атак на інформаційні системи, але найбільш небезпечною являється APT (цільова, таргетована) атака. APT атака (скорочено від англ. Advanced persistent threat) – це неперервний процес несанкціонованої активності в інфраструктурі атакованої системи, віддалено керованої вручну в реальному часі. Для реалізації атаки даного виду використовується комбінація утиліт, зловмисного ПЗ, механізмів використання вразливостей «нульового дня», інших компонентів спеціально розроблених для атаки [1]. APT відноситься до загроз зі складним рівнем знань і значними ресурсами, які можуть застосовувати декілька різних векторів атак для досягнення власних цілей, включно зі створенням плацдармів у інфраструктурі інформаційних технологій організацій для постійної крадіжки інформації та/або підриву чи перепоні критичним аспектам місії, програми чи організації або для набуття можливості виконати ці дії в майбутньому [2].

Ключовими характеристиками APT атак є:

- конкретні та чіткі цілі;
- високоорганізовані і добре забезпечені ресурсами зловмисники;
- довготривала кампанія з повторними спробами;
- використання технік приховування слідів перебування.

Розглянемо усі ключові характеристики більш детально.

Конкретні та чіткі цілі. Атаки APT - це цільові атаки, які завжди мають чітку мету. Цілями зазвичай є уряди або організації з критично важливою інфраструктурою. Зазвичай атаки спрямовані на такі галузеві вертикалі: державні, фінанси, високотехнологічні, телекомунікаційні, енергетичні, консалтингові, хімічні, медичні, освітня та аерокосмічні галузі. Поки традиційні атаки

поширюються якомога ширше, щоб поліпшити шанси на успіх і максимізувати врожай, атака APT фокусується лише на своїх заздалегідь визначених цілях, обмежуючи дальність атаки.

Що стосується цілей атаки, APT зазвичай шукають цифрові активи, що приносять конкурентні переваги або стратегічні переваги, такі як дані національної безпеки, інтелектуальна власність, комерційна таємниця тощо, тоді як традиційні загрози здебільшого шукають особисту інформацію, таку як дані кредитних карток, або загалом цінна інформація, яка сприяє фінансовій вигоди.

Високоорганізовані і добре забезпечені ресурсами зловмисники. Діючі особи, що стоять за APT, як правило, є групою кваліфікованих хакерів, які працюють злагоджено. Вони можуть працювати в урядовому/військовому кібер-підрозділі, або можуть бути найнятими у якості кібер-злочинців урядами та приватними компаніями. Вони мають достатні ресурси як з фінансової, так і з технічної точки зору. Це надає їм можливість працювати протягом тривалого періоду та мати доступ (шляхом розробки або закупівлі) до вразливостей нульового дня та інструментів атаки. Якщо вони фінансуються державою, то можуть навіть діяти за підтримки військової або державної розвідки.

Довготривала кампанія з повторними спробами. Атака APT - як правило, є довготривалою кампанією, яка може залишатися не виявленою в мережі підприємства протягом декількох місяців або років, у зв'язку з тим, що зловмисники використовують техніки приховування слідів. Зловмисники наполегливо атакують свої цілі, і вони неодноразово змінюють техніки нападу, щоб завершити роботу, коли попередня спроба не вдається.

Це відрізняється від традиційних загроз, оскільки традиційні зловмисники часто націлюються на широке коло жертв, і вони змінюють ціль, якщо не зможуть проникнути до початкової.

Використання технік приховування слідів перебування. Атаки APT є схованими, вони мають здатність залишатися непоміченими, приховуючи себе в межах корпоративного мережевого трафіку та взаємодіють настільки, щоб досягти визначених цілей. Наприклад, виконавці APT можуть використовувати експлойти

нульового дня, щоб уникнути виявлення на основі сигнатур, та шифрування, щоб ускладнити виявлення нелегітимного мережевого трафіку.

У таблиці 1.1 наведено відмінності між традиційними та APT загрозами для декількох атрибутів атак.[3]

Таблиця 1.1

Порівняння традиційних та APT атак

	Традиційні атаки	**APT атаки**
Зловмисники	Зазвичай одна особа	Добре організована, професійна, рішуча та забезпечена ресурсами група
Ціль	Неспеціалізовані, переважно індивідуальні системи	Конкретні організації, урядові установи, комерційні підприємства
Мета	Фінансова вигода, демонстрація можливостей	Конкурентні та стратегічні переваги
Підхід	Однобічний, «розбий і схопи», короткий період часу	Повторні спроби, залишає сліди низької активності, пристосовується протистояти захисту, довгострокові

1.2 Стадії розвитку APT атаки

Одну з перших поширених моделей APT-атак в 2011 запропонували працівники компанії Lockheed Martin [4]. Вони ввели новий термін Cyber KillChain, який був частиною їх моделі Intelligence Driven Defense [5] для ідентифікації та запобігання процесам кібер-вторгнення.

Ця модель є візуалізацією усіх стадій розвитку APT атаки, які необхідно виконати для її успішного здійснення. Модель KillChain використовується не тільки для розуміння дій противника, а також для побудови системи захисту аби протидіяти та захистити інформаційні ресурси підприємства.

Модель складається з 7 основних етапів: розвідка, озброєння, доставка, зараження, інсталяція, отримання управління, виконання дій (рис.1.1).

Рисунок 1.1 – Модель KillChain

Перед початком розгортання моделі KillChain для певної цілі, цю саму ціль необхідно обрати. Ціллю для атаки може стати будь-яка організація, але, найбільш цікавими являються такі частини підприємства:

- офіс правління;
- науково-дослідні та дослідно-конструкторські роботи;

- центри обробки даних;
- мережа постачальників;
- системи хмарних обчислень;
- виробництво;
- бази даних, в яких зберігається критична інформація для підприємства.

Розвідка. Розвідка також відома як збір інформації, що є важливим етапом підготовки до початку атак. На цьому етапі зловмисники визначають та вивчають цільову організацію, збираючи якомога більше інформації про технічне середовище та ключовий персонал цієї організації [3]. На даній стадії важливі усі деталі, які допоможуть виявити потенційні слабкі місця. У роботі можуть бути використані найнетривіальніші підходи для отримання закритої конфіденційної інформації. Ця інформація часто збирається за допомогою інсайдерів, пошуку за відкритими джералами (OSINT) та методів соціальної інженерії.

- Інсайдери. Існує підхід з пошуком недавно звільнених співробітників підприємства. Колишній співробітник отримує запрошення на звичайну співбесіду на дуже заманливу позицію. Відомий факт, що досвідчений психолог-рекрутер може розговорити будь-якого співробітника, який бореться за позицію. Від таких людей отримують достатньо великий обсяг інформації для підготовки і вибору вектора атаки: від топології мережі і використовуваних засобів захисту до інформації про особисте життя інших співробітників [1].

- Соціальна інженерія. Соціальна інженерія – це сукупність психологічних і соціологічних прийомів, методів та технологій, які дозволяють отримати конфіденційну інформацію [6]. У кібер-атаках соцінженерія часто використовується для отримання конфіденційної інформації або отримання цілі для здійснення певних дій (наприклад, виконання шкідливих програм). Наприклад, у випадку телефонного дзвінку зловмисник представляється від імені робітника інформаційної служби, задає правильні питання чи просить виконати потрібну команду на комп'ютері.

- OSINT. OSINT - це форма збору розвідувальних даних із загальнодоступних джерел, і в наш час вона, як правило, відноситься до збору інформації про ціль за

допомогою платних або безкоштовних джерел в Інтернеті. За допомогою OSINT можна збирати різну інформацію, починаючи від особистого профілю працівника і закінчуючи конфігураціями апаратного та програмного забезпечення в організації.

Також цінним джерелом отримання інформації являються державні портали закупівель. Там можна знайти інформацію про рішення, які впроваджені у замовника, в тому числі про системи захисту інформації. На перший погляд цей приклад може бути не значним, але насправді це не так. Перерахована інформація приміняється в методах соціальної інженерії, дозволяючи хакеру легко завоювати довіру, оперуючи отриманою інформацію. Додатково зловмисниками використовується недобросовістне відношення підприємств до паперових носіїв інформації, які викидають на смітник без правильної утилізації, серед сміття можуть бути знайдені звіти та внутрішня інформація, чи, наприклад, сайти компаній, які містять реальні імена співробітниківв загальному доступі. Отримані дані можна буде комбінувати з іншими техніками соціальної інженерії.

Озброєння. На основі зібраних розвідувальних даних учасники APT атаки складають стратегію нападу та готують необхідні інструменти. Стратегія нападу є обов'язковою в реалізації успішної атаки, вона враховує весь план дій на усіх стадіях атаки:

- описання етапів атаки: від озброєння до виконання дій;
- методи соціальної інженерії, використовувані вразливості, обхід стандартних засобів безпеки;
- етапи розвитку атаки з урахуванням усіх можливих внештатних ситуацій;
- закріплення всередині, підвищення привілегій, контроль над ключовими ресурсами;
- вилучення даних, видалення слідів, деструктивні дії.

Для успіху зловмисники зазвичай готують різні інструменти для різних векторів атак, щоб вони могли адаптувати тактику на випадок невдачі. Перед зловмисниками встає непростий вибір: необхідно обрати між фінансовими

витратами на купівлю уже готових інструментів на «тіньовому» ринку чи затратами праці та часу на створення власних інструментів. «Тіньовий» ринок надає досить широкий вибір різних інструментів, що значно скорочує час, за випадком унікальних ситуацій.

Якщо розглянути набір інструментів зловмисників, то, як правило, він включає три основні компоненти:

1. командний центр (Command and Control Center). Основою інфраструктури зловмисників є командно-контрольні центри, що забезпечують передачу команд підконтрольним зловмисним модулям, з яких збирають результати роботи. Центром атаки являються люди, що проводять атаку. Найчастіше центри розташовуються в інтернеті у провайдерів, що надають послуги хостингу, колокації та аренди віртуальних машин. Алгоритм оновлення, як і усі алгоритми взаємодії з «господарями», можуть змінюватися динамічно разом зі зловмисними модулями;

2. інструменти проникнення. Наступні засоби вирішують задачу «відкриття двері» атакованої віддаленної кінцевої точки:

- експлойт (від англ. exploit) – зловмисний код, що використовує вразливості в програмному забезпеченні.
- валідатор – зловмисний код, що застосовується у випадку першого інфікування, що має можливість зібрати інформацію про кінцеву точку, передати її командному центру для подальшого прийняття рішення про розвиток атаки чи повної її відміни на конкретній машині.
- завантажувач (від англ. downloader) модуля доставки Dropper. Завантажувач досить часто використовується в атаках, що побудовані на методах соціальної інженерії, відправляється вкладенням у електронних поштових повідомленнях.
- модуль доставки Dropper. Зловмисна програма (як правило, вірус типу «Троянський кінь»), задачею якої є доставка основного вірусу Payload на інфіковану машину жертви та призначений для закріплення всередині інфікованої машини, прихованого автоматичного завантаження, інжектування процесів після

перезавантаження машини, а також для включення в легітимний процес для завантаження і активації вірусу Payload зашифрованим каналом або для вилучення і запуску шифрованої копії вірусу Payload з диску. Виконання коду відбувається в інжектованому легітимному процесі з системними правами, така активність досить важку виявляється стандартними засобами безпеки;

3. тіло вірусу Payload. Основний зловмисний модуль у атаці, що завантажується на інфікований хост, може складатися з декількох функціональних додаткових модулів, кожний з яких буде виконувати свою функцію:

- клавіатурний шпигун;
- запис екрану;
- віддалений доступ;
- модуль поширення всередині інфраструктури;
- взаємодія з командним центром та оновлення;
- шифрування;
- очищення слідів активності, самознищення;
- читання локальної пошти;
- пошук інформації на диску.

Потенціал розглянутого набору інструментів високий, а функціонал модулей і використовуваних технік може сильно відрізнятися в залежності від планів атаки.

Доставка. На цьому етапі зловмисники доставляють свої експлойти до цілей. Існує два типи механізмів доставки: пряма та непряма доставка. Для прямої доставки зловмисники надсилають експлойти до своїх цілей за допомогою різних технологій соціальної інженерії, таких як цільовий фішинг.

Непряма доставка є крадіжкою. При такому підході зловмисники компрометують третю сторону, якій довіряє ціль, а потім використовують скомпрометовану третю сторону для опосередкованого обслуговування експлойтів. Довірена третя сторона може бути постачальником програмного / апаратного забезпечення, що використовується в цільовій організації, або законним веб-сайтом, який часто відвідують цільові особи (атака watering hole).

- Цільовий фішинг. Цільовий фішинг - це форма фішингу, при якій шахрайські електронні листи спрямовані лише на невелику групу вибраних одержувачів. Зазвичай він використовує інформацію, зібрану під час розвідки, щоб зробити атаку більш конкретною та «особистою» для цілі, щоб збільшити ймовірність успіху. Одержувача спокушають або завантажити, здавалося б, нешкідливе вкладення, що містить експлойт вразливості, або клацнути посилання на шкідливий веб-сайт, що обслуговує експлойти, що накопичуються при завантаженні. При APT атаках зловмисні вкладення використовуються частіше, ніж шкідливі посилання, оскільки люди зазвичай діляться файлами (наприклад, звітами, діловими документами та резюме) електронною поштою в корпоративному чи державному середовищі.

- Атака watering hole. Поняття нападу watering hole схоже на хижака, який чекає біля водопою в пустелі, оскільки хижак знає, що жертвам доведеться підійти до водопою. Подібним чином, замість того, щоб активно надсилати зловмисні електронні листи, зловмисники можуть ідентифікувати веб-сайти третіх сторін, які часто відвідують цільові особи, а потім спробувати заразити один або кілька з цих веб-сайтів шкідливим програмним забезпеченням. Зрештою, доставка здійснюється, коли заражені веб-сторінки переглядають жертви. Використання атаки watering hole були помічені в декількох кампаніях APT. Наприклад, такий тип доставки було використано при атаці NotPetya та атаці на Міжнародну організацію цивільної авіації в Монреалі в 2017 році, а також в кампанії Holy Water у 2019 році.

Наведені механізми доставки не були би ефективними, якби зловмисники не удосконалювали способи маскування експлойтів, що доставляються цілі. Оскільки на сьогоднішній день стандартні рішення інформаційної безпеки налічують величезну кількість функцій, що забезпечують високий рівень з контролю і фільтрації даних, то кіберзлочинці вдаються до наступних методів обману захисних механізмів системи:

- обфускація коду. Заплутування коду на рівні алгоритму за допомогою спеціальних компіляторів для ускладнення його аналізу антивірусним програмним забезпеченням;

- шифрування. Багаторівневе шифрування застосовується для приховування частини коду від детектуючих механізмів. Часто обфускація застосовується разом з частинним багаторівневим шифруванням коду;
- інжектування процесу. Техніка з динамічного впровадження власного коду в чужий процес. Дозволяє використовувати усі привілегії легітимного процесу у власних цілях, не привертаючи уваги встановлених механізмів захисту. Даний метод дозволяє обійти різні системи контролю безпеки, у тому числі і контролю додатків. Інжектування відбувається на рівні Windows API: визначення дескриптору необхідного процесу, а потім створення нового потоку в віртуальному середовищі процесу;
- mimikatz. Інструмент перехоплення паролей відкритих сесій у Windows, що реалізує функціонал Windows Credential Editor. Може витягувати аутентифікаційні дані користувача, що аутентифікувався в системі, у відкритому вигляді;
- руткіт. Даний інструмент використовується для обходу захисту, закріплення у взламаній системі і приховування слідів присутності. Для Unix-систем пакет утиліт (який містить також сканер, сніфер, кейлогер) включає в себе і троянські програми , які замінюють собою основні утиліти Unix. Для Windows пакет перехоплює і модифікує низькорівневі API-функції, дозволяючи маскувати свою присутність в системі (приховуючи процеси, файли на диску, ключі в реєстрі). Багато руткітів встановлюють свої драйвери і служби. Руткіт також може бути використаний як інструмент доставки, що може вивантажити все необхідне зловмиснику після зараження машини;
- обхід емулятора. Антивірусний емулятор перевіряє виконуваний файл в ізольованому середовищі, аналізуючи логіку його роботи. Виявлення зловмисного коду відбувається сигнатурним чи евристичним методом. Зловмисники використовують різні практики з використання алгоритму коду, не дозволяючи емулятору виявити логіку виконання зловмисної програми;

- обхід поведінкового аналізу. Такий метод детектування використовується пісочницею в цілях виявлення загроз нульового дня. Так як час перевірки пісочницею обмежено її функціональними можливостями, зловмисники використовують затримувач, і виконуваний код «засипає» на деякий час, щоб заопбігти виявлення [7].

Зараження. Зараження відбувається, коли зловмисник отримує перший несанкціонований доступ до комп'ютера/мережі цілі. Хоча зловмисники можуть отримати облікові дані доступу за допомогою соціальної інженерії та просто використовувати їх для несанкціонованого доступу, типовим способом вторгнення є виконання шкідливого коду, який використовує вразливість на комп'ютері цілі. Зловмисники спочатку доставляють зловмисний код на етапі доставки, а потім на етапі вторгнення отримують доступ до цільового комп'ютера, коли експлойт успішно виконаний.

Задля того аби успішно виконати зараження необхідно знайти вразливості у програмному забезпеченні. Вразливості ПЗ можна розділити на два основні типи:

- відомі – вразливості, що мають стандартно класифіковний CVE (від англ. Common Vulnerabilities and Exposures) опис і готові виправлення в оновленнях розробника;
- невідомі, або вразливості нульового дня, не виправлені і ще не виявлені розробниками і дослідниками загрози. Такого роду загрози є гарним заробітком для «чорних» хакерів , що заробляють на продвжі виявлених вразливостей на хакерських ринках.

Яскравим прикладом експлуатації вразливостей в процесі проникнення в інфраструктуру являється:

- переповнення буферу - може викликати аварійне завершення чи зависання програми (відмовлення в обслуговуванні). Окремі види переповнення дозволяють зловмиснику завантажити і виконати довільний код від імені програми і с правами облікового запису, під яким ця програма була запущена. Наприклад, користувач з правами адміністратора на своєму комп'ютері може отримати лист з

владеним PDF-документом, в який буде «вшито» експлойт. При відкритті чи попередньому перегляді вкладеного документу запуститься процес переповнення буферу, що дозволяє злоумиснику отримати права локального адміністратора на цьому комп'ютері;

- USB-пристрої в поєднанні з вразливістю та методом соціальної інженерії. Приклад зараження через підключення USB-пристроя досить простий в реалізації. Наприклад, відомі випадки, коли в офісі компанії (на парковці, біля входу, біля ліфту) були розкидані інфіковані USB-пристрої з документом під інтригуючою для простого співробітника назвою (річний звіт, фінансовий план) в який «вшито» експлойт [7].

При атаках APT зловмисники часто зосереджуються на вразливостях в таких програмних продуктах як Adobe PDF, Adobe Flash та Microsoft Office, а також Internet Explorer.

Зараження є ключовою фазою в APT атаці, починаючи з цієї стадії актори APT закріплюються в мережі цілі. Успішне зараження, як правило, призводить до встановлення шкідливого програмного забезпечення. З цього моменту зловмисники підключаються до мережі цілей.

Інсталяція. На стадії інсталяції зловмисники вже мають адміністративні права і всі їх дії по відношенню до систем безпеки абсолютно легальні. Використовуючи стандартні інструменти віддаленого доступу, вони обирають найбільш зручні з точки зору поставлених задач сервери та робочі станції. Для успішного проходження цієї стадії необхідно виконати 3 основних кроки.

Крок 1. Закріплення всередені інфраструктури. Під закріпленням мається на увазі комплекс дій, що направлені на організацію гарантованого доступу в інфраструктуру цілі. Справа в тому, що початковою точкою проникення є, як правило, комп'ютери співробітників з фіксованим робочим графіком, а це означає, що час доступу в інфраструктуру для зловмисника буде обмеженим.

Крок 2. Поширення. Значним аспектом є наявність постійних активних точок входу, зазвичай для цього використовуються сервери з малим часом простою, які

добре підходять для виконання одного з головних правил цільової атаки – «постійність». На цьому рівні для виконання зараження подальших робочих станцій/серверів необхідно підключитися до вибраної машини віддаленим RDP-клієнтом і запустити зловмисний модуль, перед цим скопіювавши його одним кліком мишки.

Крок 3. Оновлення. Буває, коли певна функція відсутня в арсеналі уже задіяного в атаці основного модуля, наприклад, такою функцією може виявитися запис звуку з зовнішнього мікрофону. Можливість оновити модуль передбачена розробниками атаки і може бути активована при необхідності [7].

Отримання управління. Зловмисник створює канал Command&Control як вхід до внутрішніх активів жертви за допомогою встановленого шкідливого програмного забезпечення. На цьому етапі зловмисник контролює машину жертви. Зловмисник використовує канал Command&Control, щоб повідомити скомпрометовану машину, що робити далі та яку інформацію збирати. Канал Command&Control може бути централізованою або одноранговою децентралізованою структурою. У централізованій структурі центральний сервер використовується для керування та управління зкомпрометованими машинами. У одноранговій децентралізованій архітектурі заражені машини використовуються як вузли, і кожен вузол відповідає лише за підмножину загальної кількості ботів у ботнетах. Деякі з методів, що використовуються шкідливим програмним забезпеченням для досягнення непомітного анонімного каналу зв'язку, включають використання Internet Relay Chat, інструментів віддаленого доступу, використання протоколів TCP / HTTP / FTP, стеганографію та використання The Onion Router (TOR) чи швидкого потоку DNS. Це лише деякі способи, якими автори шкідливих програм користуються, щоб приховати свій сервер Command&Control від виявлення [8].

Виконання дій. В заключній фазі зловмисники підходять до ключової точки цільової атаки. На цьому етапі вони можуть виконати будь-яку дію, що направлена проти цілі, що атакується. Перелічимо основні види зловмисних дій задля яких було проведено таку масштабну атаку.

Ціль 1. Крадіжка ключової інформації. Найчастіше компанії стикаються з крадіжкою інформації. В комерційній діяльності це цілий бізнес, заснований на конкуренції і великих грошах. В державних структурах це шпигунство, рідше отримання інформації, що містить конфіденційну інформацію, для наступного перепродажу. В фінансовому секторі це інформація про платіжні і білінгові системи, рахунки крупних клієнтів та інша фінансова інформація для проведення незаконних транзакцій.

Сама крадіжка відбувається максимально непомітно для систем моніторингу компанії, маскуючи мережеву активність під роботу відомого інтернет-сервісу з найменуванням домену, який сильно нагадує реальний. Зазвичай це виглядає як активна шифрована сесія, де веб-адреса часто схожа на популярні мережеві ресурси (наприклад, поштові сервіси чи сайти новин).

Ціль 2. Зміна даних. Приклад цільової атаки Metel, від якої постраждали сотні фінансових організацій: зловмисники, використовуючи контроль над платіжною системою, змінювали доступний кредит на балансі кредитної карти, тим самим дозволяючи спільнику декілька разів переводити в готівку кошти з однієї і тієї ж карти.

А у випадку кіберкрадіжки Carbanak хакери, вивчивши роботу операціоністів, діяли від імені співробітників, використовуючи онлайн-банкінг для переведення коштів на підконтрольні зловмисникам рахунки. Також вони віддалено управляли конкретними банкоматами, відправляючи команди на видачу готівки, в той час як спільник навіть не вставляв в банкомат ніяких карток.

Ціль 3. Маніпуляція з бізнес-процесами і шантаж. Наочний випадок стався з компанією Sony Pictures, що стала жертвою атаки в 2014 році. В результаті було викрадено тисячі файлів і документів, фінансових даних, а також до злочинців потрапили у руки фільми, що готувалися до прокату. В компанії розповіли, що більшість її комп’ютерів вийшло з ладу, а на екранах відображалася фраза «ми заволоділи вашими секретами». Усі дані на жорстких дисках робочих комп’ютерів були стерті , злочинці грозилися опублікувати інформацію, якщо компанія не виконає їх вимог.

Ціль 4. Знищення даних. Цей варіант не часто зустрічається в розвитку атаки, але в серпні 2012 року близько 30 тисяч персональних комп'ютерів , що належали одній з найбільших в світі компанії з видобутку нафти Saudi Aramco, були виведені з ладу. У злочинців було дві мети: перша – крадіжка закритої інформації, друга – повна зупинка бізнес-процесів компанії . В результаті атаки компанія була вимушена майже на місяць припинити свою операційну діяльність, відімкнувши філіали від мережі Інтернет.

Протягом усієї атаки зловмисники намагаються маскувати свою присутність під легітимний процес, в крайніх випадках, коли це не можливо, хакери вручну очищують журнали подій. Як правило, більша частина активності протікає під адміністративним доступом, не викликаючи підозр.

Завершуючи фінальну стадію атаки більшість зловмисників намагаються залишити всередині інструмент, що дозволить в разі необхідності повернутися знову в інфраструктуру. Таким інструментом зазвичай є керований завантажувач, що за командою може завантажити виконуваний модуль [7].

1.3 Методи протидії APT атакам

APT атаки з часом стають все більш досконалими та сильнішими. Через складність та невидимість атак, не існує єдиного рішення, яке пропонує ефективний захист. Сучасна найкраща практика - це широкий спектр заходів протидії атакам, що є наслідками багаторівневої оборони. В даний час одними з найкращих доступних засобів захисту від APT атаки є ряд загальноприйнятих технік, таких як:

- брандмауери;
- система виявлення вторгнень (IDS);
- система запобігання вторгнень (IPS);
- пісочниця (sandbox);
- брандмауер WEB-додатків;
- захист електронної пошти;

- антивіруси.

З огляду на швидке вдосконалення APT атак, зазначені інструменти не надто ефективні, і необхідні нові методи, такі як багатошарова система оборони.

Глибинний захист / багатошарова система оборони

Глибинний захист (від англ. defense in depth) - це багатошаровий захисний метод, який базується на концепції військової дисципліни. Основна ідея полягає у застосуванні захисної системи на декількох рівнях мережі, що робить її набагато безпечнішою порівняно з одношаровим механізмом захисту. Поглиблений захист не тільки захищає систему від APT атак, але також може надати цінну інформацію про атаку та зловмисника. Така інформація може не тільки допомогти у відстеженні зловмисника, але й може допомогти мінімізувати шкоду, заподіяну APT атакою, що є дуже корисним механізмом, оскільки зазвичай виявити атаку досить складно, але ще складніше відстежувати шкоду, заподіяну атакою. У таблиці 1.2 показано ілюстрацію логічного підходу до системи глибинного захисту на основі шарів [9].

Таблиця 1.2

Глибинний захист проти APT атак

Шари	**Методи захисту**
Ідентифікація та доступ	Управління ідентифікацією та доступом (IaAM)
Фізичний	Фізична безпека
Мережевий	1. Система виявлення та запобігання вторгнень 2. Безпека VOIP 3. Сегментація мережі та брандмауер 4. Інспекція вмісту Інтернету та пошти 5. Захищений віддалений доступ 6. Шифрування даних 7. Контроль доступу до мережі
Операційна система	Захист операційної системи
Додатки	Брандмауер додатків
Дані	Захист баз даних

Оскільки підхід глибинного захист - це комбінація засобів захисту, як показано в таблиці 3, яка забезпечує комплексний захист від нових та вдосконалених APT атак. Глибинний захист працює на загальному підході до захисту всіх активів, беручи до уваги взаємозв'язки та залежності активів, а також реалізує наявні ресурси в ефективній системі моніторингу та захисту, тим самими мінімізуючи вплив бізнесу на ризики кібербезпеки. Вичерпний виклад інструментів та прийомів, які використовує глибинний захист, наведено в таблиці 1.3.

Таблиця 1.3

Елементи захисту при використанні методу Defense in depth

Програма ризик-менеджменту	1. Визначення загроз 2. Характеризування ризиків 3. Інвентаризація активів
Архітектура кіберзахисту	1. Стандарти / рекомендації 2. Політика 3. Процедури
Фізична безпека	1. Контроль доступу до Центру управління 2. Віддалене відео сайту, засоби контролю доступу, бар'єри
Мережева архітектура	1. Спільні архітектурні зони 2. Демілітаризовані зони (DMZ) 3. Віртуальні локальні мережі
Безпека мережевого периметру	1. Брандмауери 2. Віддалений доступ та аутентифікація 3. Сервери переходу
Безпека кінцевих точок	1. Управління виправленнями та вразливостями 2. Віртуальні машини
Моніторинг безпеки	1. Системи виявлення вторгнень 2. Ведення журналу аудиту безпеки 3. Моніторинг аварій та подій безпеки
Управління постачальниками	1. Управління ланцюгами поставок 2. Керовані послуги / аутсорсинг 3. Використання хмарних служб

Людський фактор	1. Політика 2. Процедури 3. Навчання та обізнаність

З таблиць 1.2 та 1.3 цілком зрозуміло, що техніка глибинного захисту дуже схожа на техніку розгортання APT атаки, оскільки APT атака - це також поєднання різних інструментів, що використовуються на різних фазах атаки, що ускладнює її виявлення. Застосовуючи подібний підхід, глибинний захист застосовує цілісну тактику для захисту системи від APT атак. Представлена техніка не є єдиним механізмом, але це група різноманітних інструментів, таких як; люди, технології, стандартні процедури безпеки, операції та інформування організацій. Основна мета техніки глибинного захисту - збільшення шансів уникнення APT атаки та забезпечення комплексного методу відновлення та відстеження у випадку, якщо атака матиме успіх у доступі до мережі підприємства.

Оборонні методики, запропоновані дослідженнями і організаціями безпеки

Підхід, що базується на багатошаровості, не єдина протидія проти APT атак, експерти з безпеки та організації, запропонували також інші комплексні методи. У таблиці 1.4 містяться методи, запропоновані найбільш відомими організаціями, що реалізують безпеку, для протидії APT атакам.

Таблиця 1.4

Методи захисту від APT атак, запропоновані відомими організаціями безпеки

Назва дослідження	**Метод атаки**	**Метод захисту**
Advanced Persistent Threats: A Symantec Perspective	Відповідно до статті, метод APT-атак поділяється на 4 фази: вторгнення в мережу, виявлення цілі, захоплення цільових даних та вихід з мережі. Атаки розпочинаються через фішинг електронної пошти, зловмисне програмне забезпечення, яке стоїть за	Відповідно до статті, такі атаки можна запобігти шляхом реалізації: 1 - Засоби безпеки, засновані на поведінковому аналізі, такі як антивірус та брандмауери. 2 - Ретельний моніторинг та фільтрація вхідного та вихідного трафіку. 3 - Впровадження шифрування

	рекламними кліками, пошук вразливостей у мережі, збір бажаних даних та видалення слідів.	даних та використання VPN.

Продовження табл. 1.4

Defending Against Advanced Persistent Threats: Strategies for New Era of Attack	Стаття заснована на дослідженні, проведеному CA Technologies. Відповідно до дослідження, APT атаки, як правило, проводяться на транснаціональні компанії з великими даними або високою цінністю в умовах ринкової вартості. У цій роботі автори описують зловмисника як того, хто завжди шукає вразливість для проникнення в мережу, після успішної інфільтрації зловмисник запускає протоколи виявлення, щоб дізнатися деталі мережі. Такі деталі можуть включати інформацію про порти, використовуючи сканування портів або маршрути руху інформації. Після збору такої інформації зловмисник шукає потрібні дані, не викликаючи жодних підозр. Як тільки ціль виявлена, зловмисник захоплює дані та виходить із мережі. У разі успішної атаки компанії зі спільною політикою управління зазнають більших втрат. Крім того, компрометована мережа може надати зловмиснику системні журнали, паролі користувача, а в деяких випадках зловмисник	Автори статті пропонують наступні методи для того, щоб протидіяти атаці: 1 - Блокування будь-яких невикористовуваних портів. 2 - Шифрування даних принаймні 128 бітами хешу MD5. 3 - З метою аудиту журнал повинен зберігатися і час від часу перевіряти на наявність підозрілої діяльності. 4 - Для захисту сеансів слід застосувати наскрізний антивірус. 5 - Чітке визначення політики брандмауера для зіткнення з атаками з внутрішніх та зовнішніх джерел. Дослідження показують, що велика кількість кібератак проводиться з внутрішньою допомогою; щоб уникнути таких інцидентів, необхідно виконати наступне: 1 - Аккаунти слід надійно зберігати у різних віртуальних мережах, а привілеї користувачам надавати лише за необхідністю. 2- Аккаунти, що належать працівнику, який більше не є частиною організації, слід негайно видаляти.

Продовження табл. 1.4

	залишає в мережі інструмент для повернення.	
Countering the Advanced Persistent Threat Challenge with Deep Discovery	Дані, використані в цій роботі, зібрані від Trend Micro; стаття вказує, що APT атаки в будь-якій організації - це знищення мережі, а також організації. Дослідження також вказує на те, що APT атака може легко порушити традиційні захисні системи, такі як брандмауер або антивірус. Опис зловмисника у цій роботі повністю відповідає опису попередніх робіт. Як тільки зловмисник отримує інформацію про цільову мережу та точку входу зловмисник бомбардує мережу	Автори статті пропонують такі методи запобігання атакам: 1 - Використання протоколів SSL / SSH, щоб уникнути завантаження будь-якого зараженого файлу або перенаправлення браузера на шкідливі сайти, 2 - Впровадити стратегію пісочниці в кінці сервера, щоб змоделювати поведінку файлів належним чином перед використанням, оновленням або реалізацією. 3 - Використання евристичних інструментів та алгоритмів для складання чорного списку IP щодо
	всіма наявними в своєму розпорядженні арсеналом, щоб створити структуру зв'язку, яка може надати йому інформацію. Як тільки це завдання досягнуто, здійснюється пошук у мережі цільових даних, які потім буде отримано та відправлено назад до штабу зловмисника. Врешті-решт зловмисник здійснює втечу, не залишаючи слідів.	підозрілої поведінки, процедур та підпрограм. 4 - Правильна конфігурація та встановлення охоронних пристроїв, контрольних пунктів та інструментів. 5 - Окремі брандмауери, які слід застосовувати на кожному сервері. 6 - Використання високоефективних методів шифрування даних. Якщо дані будуть скомпрометовані, розшифрувати їх буде непростим завданням.

Продовження табл. 1.4

The Study of APT Attack Stage Model	Відповідно до дослідження APT атаку можна розділити на 4 етапи: етап підготовки, етап доступу, етап знаходження в системі та етап збирання. Незважаючи на різні назви, концепція етапів атаки APT така ж, як описана в попередніх роботах. Початкові етапи складаються з збору інформації (прямого або непрямого), такого як сканування портів, сканування вразливості, пошукові системи, а також вдосконалені сканери та власні розробки для отримання інформації про мережу. Після отримання інформації стадія доступу виконується на основі зібраної інформації. Доступ до мережі може бути здійснений численними способами, такими як електронна пошта завдяки фішингу. Потрапляючи всередину мережі, зловмисник має намір створити механізм управління для пошуку бажаних даних, отримання їх, а потім виходу з мережі. 19% випадків APT використовують вразливості Zero Day, а майже 70% наявні вразливості.	З метою запобігання нападу APT автори цієї статті пропонують наступні кроки: 1 - Навчання персоналу. Персонал повинен знати, як запобігти витоку даних через соціальні медіа, а також нікому не передавати інформацію про аутентифікацію. 2 - Правильна реакція на безпеку внутрішньої мережі. 3 - Постійне оновлювання системи та програмного забезпечення, щоб запобігти експлуатування вразливостей «нульового» дня. 4 - Брандмауери повинні бути налаштовані належним чином, щоб доступ до мережі та вихід з неї дозволявся лише автентичному трафіку. 5 - Антивіруси слід встановлювати не тільки на базовій системі (серверах), але і на кожній кінцевій точці. 6 - Впровадження системи IDS , яка може попереджати про будь-які підозрілі дії. 7 - Розроблення та використання суворої політики безпеки відповідно до стандартів. 8 - Розгортання в мережі інструментів, типу honey pots з метою виявлення підозрілої чи шкідливої активності.

Продовження табл. 1.4

		9 - Використання пісочниці для перевірки підозрілого файлу перед його запуском. 10 - Експерти з безпеки повинні пройти оцінку ризику, якщо атака APT успішно проводиться або триває в мережі.

Інструменти поведінкового аналізу для виявлення APT атак

У цьому розділі розглядаються інструменти, які можна використовувати для виявлення APT атаки. У таблиці 1.5 наведено перелік інструментів, які можна ефективно використовувати для виявлення APT атаки у мережі. Ці інструменти мають два основних аналітичні методи виявлення відхилень у мережі. Згадані засоби можуть виявити атаку на основі поведінки мережі та кодування програми, яка працює в мережі.

Таблиця 1.5

Інструменти поведінкового аналізу та кодування для виявлення APT атаки

Інструмент	**Опис**	**Аналітичний метод**
Autoruns	Надає список розташувань файлів із автоматичним запуском.	Поведінковий аналіз
Process Monitor	Реєструє зміни в будь-якому реєстрі, файлі, процесі, потоці тощо.	Поведінковий аналіз
ListDLLs	Надає список DLL-файлів у системі.	Поведінковий аналіз
TCPView	Відстеження або реєстрація активних наскрізних з'єднань TCP/UDP	Поведінковий аналіз
VMmap	Надає детальну інформацію щодо віртуальної та фізичної пам’яті, яка використовується будь-якою	Поведінковий аналіз

	програмою	

Продовження табл. 1.5

CaptureBat	Сервіс Honeypot на кінцевій точці для реєстрації та відстеження будь-яких атак.	Поведінковий аналіз
Wireshart	Аналізатор пакетів та мережевих протоколів	Поведінковий аналіз
REMnux	Службовий інструмент на базі Linux для аналізу будь-якого шкідливого програмного забезпечення та його зворотного проектування.	Поведінковий аналіз / Кодування
FileInsigh	Службове програмне забезпечення для відображення файлів як у текстовому, так і в шістнадцятковому форматі	Кодування

Такі інструменти можуть бути дуже ефективними, але в активній мережі виявити будь-які відхилення, особливо коли мережа має тисячі вузлів та користувачів з величезною кількістю транзакцій даних додатків в секунду, постає величезною складністю [9].

Висновки за розділом 1

Проаналізовано характерні особливості, стадії розвитку та способи захисту від APT атак.

Розглянуто критерії, які вирізняють атаки APT в окремий підвид атак на інформаційні системи : конкретні та чіткі цілі; високоорганізовані і добре забезпечені ресурсами зловмисники; довготривала кампанія з повторними спробами; використання технік приховування слідів перебування. Наведені характеристики приведено на основі діяльності світових APT-груп. Також надано ключові відмінності між традиційними та APT атаками.

Приведено стадії розгортання атаки за моделлю Cyber Kill Chain, яка на сьогоднішній день найповніше описує життєвий цикл атаки, який складається з 7 основних етапів: розвідка, озброєння, доставка, зараження, інсталяція, отримання управління та виконання дій. При детальному аналізі кожного етапу виявлено, що для успішного виконання необхідне застосування великої кількості технік та методів, які роблять кожну атаку унікальною.

Надалі розглянуто передові світові практики щодо захисту/виявлення APT атак. Визначено три основні стратегії захисту: технологія defense in depth, так званого глибинного захисту; методи, запропоновані організаціями безпеки, такими як Symantec, CA Technologies та інші; інструменти поведінкового аналізу. Варто зазначити, що найдоцільнішим рішенням захисту є комбінація приведених стратегій.

З усього вище наведеного можна зробити висновок, що APT атаки є неймовірно серйозною загрозою для великих підприємств, яка приносить величезні грошові втрати (плата за розблокування мережі, відновлення працездатності, покращення механізмів захисту, відновлення втрачених матеріалів), але при продуманій оборонній стратегії та якісній роботі співробітників можна істотно мінімізувати ризики проникнення зловмисників до інформаційної системи.

РОЗДІЛ 2
SECURITY OPERATIONS CENTER ТА ЙОГО КОМПОНЕНТИ

2.1 Security Operations Center

SOC (англ. Security Operations Center), центр оперативного реагування на інциденти інформаційної безпеки – це організаційна одиниця підрозділу інформаційної безпеки, що об'єднує в собі людей, процеси та технології, яка необхідна для отримання ситуаційної обізнаності в процесі виявлення, локалізації і запобігання загроз інформаційній безпеці. SOC являє собою еволюцію поняття CERT (англ. Computer Emergency Response Team) – групу реагування на надзвичайні ситуації в області інформаційних технологій. Одна з ключових особливостей – використання аналітичних технологій для створення єдиного оперативного бачення ситуації в компанії с точки зору ІБ [10].

При побудові SOC необхідно пам'ятати декілька важливих моментів. Security Operations Center – це не тільки технічні інструменти. Це команда, задача якої виявляти, аналізувати, реагувати, повідомляти про виникнення і запобігати інцидентам ІБ. Ще один важливий компонент SOC – це процеси, оскільки мається на увазі взаємодія між співробітниками підрозділу, що відповідають за моніторинг і реагування на інциденти , а також між різноманітними підрозділами (наприклад, IT та ІБ). Від того, наскільки якісно побудовані ці процеси, буде залежати ефективність роботи SOC. Технічні засоби є лиш інструментами, що дозволяють автоматизувати частину процесів, які функціонують в SOC [11]. Таким чином, формула ідеального SOC виглядає так: SOC = персонал + процеси + технічні інструменти. Основні функції SOC на основі класифікації MITRE наведені на рисунках 2.1 та 2.2.

Рисунок 2.1 – Функції SOC

Рисунок 2.2 – Функції SOC

Побудова SOC складається з декількох кроків:

- формування цілей, задач та ключових параметрів SOC;
- визначення основних процесів та процедур SOC;
- дослідження інфраструктури і вибір технічних інструментів;
- підбір персоналу та визначення режимів роботи;
- навчання співробітників;
- контроль результатів.

Формування цілей, задач та ключових параметрів SOC. Цілі створення SOC визначає команда архітекторів, керівник відділу інформаційної безпеки та керівництво підприємства. Зазвичай, основними задачами SOC є:

- активне запобігання інцидентів ІБ;
- виявлення та аналіз порушень ІБ в режимі реального часу;
- реагування на інциденти;
- забезпечення усіх зацікавлених сторін в компанії інформацією про поточний рівень ІБ.

До основних параметрів відносять:

- організаційну модель: чи інтегровано SOC в інший підрозділ та чи є він незалежним, наскільки він централізований, кому підпорядковується, яких спеціалістів може залучати для роботи;
- виконувані функції, що виходять з задач;
- рівень повноважень: повноваження SOC можуть різнитися від простих «радників» (оповіщення, надання рекомендацій) до «спецназу» (в рамках реагування на інцидент можливе конфігурування обладнання, зміна бізнес-процесів, зупинка систем) [11].

Визначення основних процесів та процедур SOC. Виділяється більш ніж 40 основних функцій, які може виконувати SOC: від збору даних про інциденти до взаємодій з правоохоронними органами, від аналізу зловмисного коду до підвищення обізнаності співробітників. Але варто зазначити, що найімовірніше систем, які б успішно виконували усі функції одночасно не існує. Тому варто

сконцентруватися на ключових задачах, які стоять перед системою, що створюється і описати процеси, що забезпечують їх виконання. Необхідно як мінімум збирати, зберігати і обробляти дані від ІБ- та ІТ-систем, надати можливість користувачам сповіщати про підозрілу активність, розслідувати та реагувати на інциденти. Команді SOC необхідно мати актуальну інформацію про інфраструктуру, яку вона захищає і ефективно взаємодіяти з колегами з інших підрозділів: ІТ- та ІБ-служби, HR, юристи, власники систем та інші. Без цього важко уявити роботу SOC, тому саме з цього і необхідно почати. Процеси та процедури краще фіксувати на папері, аби всі учасники процесу будували одне і теж.

Дослідження інфраструктури і вибір технічних інструментів. Технічні засоби необхідні для того аби автоматизувати процеси. Для цього напочатку виконують інвентаризацію ІТ- та ІБ-активів підприємства. У питані інвентаризації допомагають рішення класу Vulnerability Management чи, як прийнято їх називати, сканери вразливостей. Ці рішення допомагають в короткі терміни зібрати інформацію про наявні компоненти інфраструктури і про їх вразливості, а також в майбутньому надають можливість відстежувати появу нових компонентів в інфраструктурі підприємства.

Зібравши інформацію про наявні компоненти, необхідно поділити їх за рівнем критичності. Найкритичніші активи повинні підключатися до SIEM в першу чергу. Виходячи з набору критичних активів, варто визначитися з правилами кореляції, які вони допоможуть налаштувати. Підключення інших активів і налаштування правил кореляції для них можна відкласти на інший етап [11].

Звичайно, окрім SIEM системи для побудови SOC необхідні інші технічні засоби. Типова інфраструктура інструментів SOC зображена на рисунку 2.3.

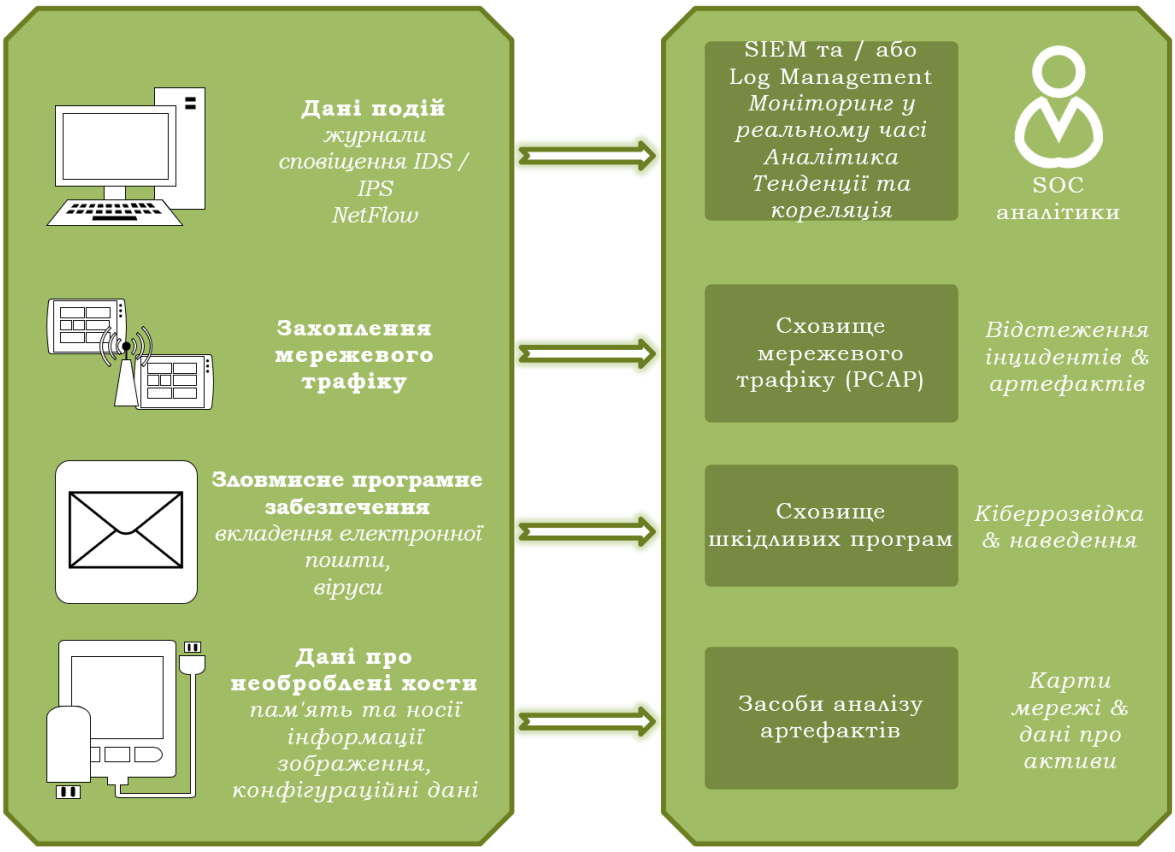

Рисунок 2.3 – Типова інфраструктура інструментів SOC

Підбір персоналу та визначення режимів роботи. Оскільки в SOC найважливішим є команда, а не технічні засоби, які працюватимуть тільки в умілих руках, тому варто виходити з принципу «якість важливіша кількості». Основу команду варто сформувати як можна раніше, аби вони брали участь у впроваджені систем та налагоджені процесів. Якщо є така можливість, варто залучити до роботи в SOC частину співробітників, що працюють в компанії та знають особливості її IT-інфраструктури та бізнес-процесів.

Для ефективної роботи варто створити групи декількох ліній. Для обробки вхідної інформації створюється група першої лінії. Вона забезпечує розбір вхідних даних і виділення у загальному потоці інформації, що відповідає прийнятим політикам даних та свідчить про інцидент ІБ. Спеціалісти першої лінії не здійснюють глибокого аналізу інциденту, їх основна задача – оперативно оброблювати вхідну інформацію. Якщо обробка інциденту займає більш ніж декілька хвилин, то інцидент повинен бути переданий на другу лінію SOC. Передачі

підлягають усі інциденти з високим рівнем критичності. Спеціалісти другої лінії можуть розслідувати інцидент від декількох хвилин до декількох тижнів, збираючи детальні дані, залучаючи експертів, відновлюючи послідовність дій і готуючи рекомендації з ліквідації наслідків інциденту, впровадження протидій та підвищенню рівня обізнаності. Корисною практикою є здійснення тимчасової ротації співробітників всередині SOC: спеціалісти другої лінії повинні частину часу працювати в першій, а спеціалісти першої лінії, в свою чергу, долучатися до розслідування частини інцидентів. Ці дії направлені на покращення якості роботи SOC, ріст професійного рівня співробітників і підвищення їх мотивації.

Ідеальний варіант режиму роботи SOC є 24/7 на повну потужність, але для більшості компанії цей графік неможливо реалізувати у зв'язку з відсутністю бажаної кількості спеціалістів чи/та нестатком коштів. Варіант 8/5 також не бажаним, оскільки багато атак відбуваються вночі. Та і такий режим не гарантує повноцінної реакції на інциденти, так як спочатку дня аналітики розбиратимуть дані за ніч (чи вихідні), а до поточних справ дійдуть лише до кінця дня, що унеможливлює оперативну обробку інформації. Тому обираючи оптимальний режим роботи формуються комбіновані варіанти. Наприклад, 12/5 з двома пересічними змінами по 8 годин в будні та по 8 годин у вихідні. Аналітики другої лінії можуть працювати при цьому в режимі 8/5. На ніч аналітичну консоль можна виводити черговій ІТ-зміні, аби вони відслідковували найкритичніші ситуації. Розуміючи витрати на той чи інший режим роботи, а також оцінюючи актуальні ризики ІБ підприємства, можна обрати найбільш оптимальну конфігурацію для кожного окремого випадку.

Навчання співробітників. Усі співробітники SOC повинні обов'язково проходити тренінги, що знайомлять їх з обов'язками, регламентами та технічними засобами. Навчання, присвячене технічним засобам, що використовується в SOC не несе на меті зробити з співробітників експертів, але дозволить швидко зорієнтуватися в складних продуктах, таких як SIEM чи сканер безпеки. Таке навчання включає в себе не тільки технічні моменти, але й процедури, індивідуальні для конкретного SOC. Збір та розповсюдження інформації всередині команди про

нові загрози і тренди ІБ повинно бути не епізодом, а налагодженим неперервним процесом. Важливим компонентом навчання є обмін досвідом всередині команди, в тому числі в рамках ротацій всередині.

Контроль результатів. Прямий підхід до оцінки результатів роботи SOC є не ефективним, так як при підвищенні якості виявлення критичних інцидентів ІБ стає більше, оскільки частина з них раніше просто не виявлялася. Аналітики отримують нові інструмент та середній час розслідування складного інциденту збільшується, але з тим зростає якість. Проте, необхідно введення ключових показників ефективності роботи, при чому не тільки для системи в цілому, але й для кожної підсистеми та співробітника. Ключові показники ефективності створюють пакет зрозумілих даних як для членів команди так і для керівництва компанії. При цьому показники повинні бути конкретні, зрозумілі, вимірювані, можливі для виконання, але амбіційні і розраховуватися за чітко визначений період часу чи до певного терміну. Прикладами ключових показників ефективності можуть бути «кількість протермінованих критичних інцидентів не більше N за місяць» чи «сумарний час простою ключової системи з вини інцидентів ІБ не більше N хвилин у квартал». Використання ключових показників ефективності дозволить швидко виявляти слабкі місця створеного SOC і вносити корегування в його роботу.

2.2 Security information and event management system

Програмне забезпечення з інформаційної безпеки та управління подіями (від англ. Security information and event management, скороч. SIEM) - це рішення безпеки, яке допомагає організаціям розпізнавати потенційні загрози безпеки та вразливі місця до того, як у них з'явиться шанс порушити ділові операції. Він виявляє аномалії поведінки користувачів і використовує штучний інтелект для автоматизації багатьох ручних процесів, пов’язаних із виявленням загрози та реагуванням на інциденти, і став основним елементом сучасних операційних центрів безпеки (SOC) для випадків використання систем безпеки та дотримання вимог [12].

Технологія SIEM існує вже більше десяти років, спочатку розвинувшись із систем управління журналами. Він поєднує управління подіями безпеки (SEM) - який аналізує дані журналу та подій у режимі реального часу для забезпечення моніторингу загроз, кореляції подій та реагування на інциденти - з управлінням інформацією безпеки (SIM), яке збирає, аналізує та звітує про дані журналів.

Програмне забезпечення SIEM збирає та узагальнює дані журналів, що генеруються по всій технологічній інфраструктурі організації, від хост-систем та додатків до мережевих та захисних пристроїв, таких як брандмауери та антивірусні фільтри.

Потім програмне забезпечення визначає та класифікує інциденти та події, а також аналізує їх. Програмне забезпечення вирішує дві основні цілі, які полягають у наданні звітів про інциденти та події, пов'язані з безпекою, такі як успішні та невдалі входи, активність шкідливого програмного забезпечення та інші можливі шкідливі дії та надсилання сповіщень, якщо аналіз показує, що діяльність працює проти заздалегідь визначених наборів правил і, отже, вказує на потенційну проблему безпеки[13].

На сучасному ринку представлена величезна кількість різноманітних продуктових рішень типу SIEM, але більшість з них мають однаковий основний функціонал. Основні функції SIEM системи представлені на рисунку 2.4.

Рисунок 2.4 – Основні функції SIEM системи

Хоча кожен постачальник пропонує унікальні особливості на ринку, можливо визначити деякі загальні риси архітектури SIEM:

- програмний компонент обробляє дані про події з одного або декількох кінцевих пристроїв; цей компонент часто називають "агентом" або "колектором", який знаходиться в одному з двох місць:
  * на пристрої, де він має прямий доступ до журналів, наприклад, через файли з розширенням CSV, або файли XML;
  * віддалено, коли він або опитує один чи декілька пристроїв для передачі даних (витягування) або приймає дані, надіслані йому (виштовхування); агент може збирати ці дані через різні власні протоколи, такі як syslog, SNMP, підключення до бази даних Java (JDBC), або в деяких випадках, власні методи, такі як виклик віддалених процедур Microsoft (наприклад, у випадку журналів Windows).
- дані збираються агентом, нормалізуються, призначається відносний пріоритет / критичність і надсилаються до SIEM, як правило, з наявними елементами управління (наприклад, сеанси SSL з автентифікацією), щоб забезпечити успішну доставку та уникнути перехоплення чи пошкодження;
- дані збираються в центральному місці. Дані можуть зберігатися в традиційній СУБД, у власній розробці бек-енд, яка підтримує високошвидкісні запити та конденсує пам'ять на диску, або через розподілену архітектуру, яка використовує методи, подібні до MapReduce;
- SIEM може зменшити обсяг даних у деяких точках своєї архітектури:
  * агрегація може бути застосована, коли кілька подій відповідають заданому набору критеріїв і зберігається лише одна. Це зменшує вимоги до зберігання, але зменшує доступні дані для подальшого використання;
  * завдяки використанню фільтрів в агенті-першоджерелі або в пункті збору SIEM небажані дані можуть бути усунені через непотрібний обсяг, повторення або відсутність цінності для аналітика;

- SIEM пропускає нормалізовані дані через механізм кореляції в режимі реального часу, використовуючи правила, націлені на різні види мережевого захисту, внутрішні загрози, відповідність нормативним вимогам та інші випадки використання для того, щоб виявити складну модель поведінки або визначити потенційні інциденти;

* деякі SIEM також дозволяють користувачеві запускати правила кореляції щодо минулих даних;

* завдяки належній нормалізації, встановленню пріоритетів та категоризації, SIEM може повністю використовувати різні канали даних, що не залежать від пристроїв;

* пріоритет подій може бути підвищено чи понижено на основі співпадінь з правилами кореляції чи порівняння з даними сканування вразливостей;

* правила кореляції можуть ініціювати різноманітні налаштовуванні користувачем дії, такі як створення випадку в SIEM і прикріплення до нього подій, запуск сценарію чи відправка аналітику електронною поштою;

- традиційно SIEM додає лише дані на основі подій, такі як NetFlow, попередження IDS та дані журналу. Він може вказувати на інші інструменти, дозволяючи аналітику запускати зовнішню скриптову команду, клацнувши правою кнопкою миші на консолі, що приведе аналітика до інструменту третьої сторони, який збирає дані сканування вразливостей, зразки шкідливих програм, телеметрію кінцевої точки або PCAP;

- деякі SIEM насправді мають можливість автоматизувати більш складні дії, що виникають внаслідок правил кореляції (наприклад, деактивація з'єднання VPN або зміна правила брандмауера). Використання таких функцій часто має ті самі наслідки, що і переведення IPS в режим активної профілактики: погано налаштовані правила кореляції можуть призвести до DoS;

- сирі та / або нормалізовані дані зберігаються, щоб забезпечити аудиторський слід та базу знань для розслідувань, аналізу закономірностей та звітування про тенденції;

- аналітики взаємодіють з даними за допомогою різних вихідних каналів, або за допомогою сповіщення про прокрутку в режимі реального часу, візуалізації подій (стовпчаста діаграма, кругова діаграма, карти подій тощо), або за допомогою статичних засобів, таких як спеціальна або запланована звітність;
- система забезпечує певний рівень реєстрації інцидентів або відстеження справ, дозволяючи користувачам підтверджувати та підсилювати як попередження, так і випадки;
- користувачі SIEM можуть переглядати вміст, створений іншими користувачами SIEM, доступ до яких контролюється за допомогою груп та дозволів, використовуючи як «запасний» вміст, що постачається постачальником, так і спеціальні звіти, правила, фільтри, інформаційні панелі та інший вміст;
- деякі найкращі у своєму роді SIEM надають способи переміщення вмісту SIEM з і до SIEM. Цю функціональність можна додатково вдосконалити за допомогою онлайн-спільнот користувачів SIEM, де користувачі можуть ділитися вмістом та співпрацювати з ним;
- кращі в своєму роді SIEM підтримують багаторівневі, однорангові / кластерні або резервні сценарії розгортання:
  * за допомогою багаторівневої структури, один SIEM може переслати деякі або всі свої дані попереджень батьківському SIEM, використовуючи той самий агент або колектор, що збирає дані від кінцевих точок;
  * за допомогою аналізу чи кластеризації кожен SIEM збирає різний набір даних, і коли користувач запускає запит, робота розподіляється по декількох SIEM, прискорюючи час запитів;
- у надлишкових сценаріях декілька екземплярів SIEM можуть приймати одні й ті самі дані, завдяки «подвійному звітуванню» від одного агенту декільком SIEM, або через синхронізацію між різними вузлами SIEM;
- у будь-якому випадку можливо масштабувати розгортання підприємств, що перевищують сотні мільйонів подій на день, одночасно надаючи аналітику значущим даним з розумним часом запитів;

Використовуючи надійну, масштабовану архітектуру та набір функцій, SIEM може підтримувати низку вагомих випадків використання:

- моніторинг периметру мережі. Класичний моніторинг обраної ділянки мережі щодо зловмисного програмного забезпечення та зовнішніх загроз;
- інсайдерська загроза та аудит. Збір та кореляція даних, які дозволяють виявляти та контролювати профілі підозрілої внутрішньої діяльності;
- виявлення APT. Складання різноманітних даних, що вказують на поперечний рух, віддалений доступ, управління та управління, а також вилучення даних;
- моніторинг конфігурації. Сповіщення про зміни конфігурації корпоративних серверів та систем, від зміни пароля до критичних змін реєстру Windows;
- робочий процес та ескалація. Відстеження подій та інциденту від початку до кінця, включаючи управління справами, встановлення пріоритетів та вирішення проблем;
- аналіз аварій та криміналістика мережі. Перегляд та збереження історії даних журналу;
- cyber intel fusion. Інтеграція самописців та сигнатур з каналів кіберрозвідки;
- трендінг. Для аналізу довгострокових закономірностей та змін у поведінці системи або мережі;
- cyber SA. Розуміння загрози в масштабах усього підприємства;
- відповідність політиці. Вбудований та настроюваний вміст, який допомагає дотримуватися законів та подавати звіти [14].

Завдяки усьому матеріалу описаному вище можна зробити наступні висновки стосовно використання SIEM систем:

- засоби забезпечення безпеки і управління мережею не є взаємозамінними. Ці інструменти мають схожу архітектуру, але виконують різні дії;

- день на встановлення, рік на введення в експлуатацію. Першочергове налаштування системи є простим і не займає багато часу, але необхідна велика кількість часу на виконання детального налаштування, що підлаштовуватиметься під особливості роботи кожного з підприємств. Паралельно відбуватиметься підвищення рівня кваліфікації співробітників, які й будуть вносити нові вдосконалення, що покращать роботу системи;
- кожна частина SOC використовуватиме SIEM по різному. Для рівня 1 необхідне сортування даних в реальному часі і конкретні випадки використання. Для рівня 2 необхідний збір якнайбільшої кількості інформації про потенційний інцидент. Для керівництва необхідний детальний звіт роботи команди безпеки. Це свідчить про те, що впроваджена SIEM слугує не лише для вузького кола спеціалістів, а пов'язує багато відділів підприємства;
- нові інструменти означають нові процеси. Варто використовувати усі наявні інструменти для роботи з даними. Для цього необхідно заново навчити співробітників поводитися з новими системами, але даний досвід значно підвищить якість обробки інформації та виведе її на новий рівень;
- SOC повинні організувати збір та зберігання інформації для підтримки кримінального, громадянського та адміністративного судочинства. Так як, електронні докази, що зібрані командою SOC з допомогою SIEM системи, можуть бути використані правозахисними органами, адвокатами і різноманітними слідчими органами у відповідь на серйозні інциденти, що призвели до порушення законодавства.

2.3 Засоби для моніторингу мережевої активності

2.3.1 Сканери вразливостей

Сканери вразливостей - це автоматизовані інструменти, що дозволяють організаціям перевіряти, чи є в їх мережах, системах і додатках слабкі місця в

системі безпеки, які можуть піддати їх атакам. Сканування вразливостей є звичайною практикою в корпоративних мережах і часто пропонується галузевими стандартами і урядовими постановами для підвищення рівня безпеки організації.

У сфері сканування вразливостей існує безліч інструментів і продуктів, які охоплюють різні типи активів і пропонують додаткові функції, які допомагають організаціям реалізувати повну програму управління вразливостями - сукупність процесів, пов'язаних з виявленням, класифікацією і усуненням вразливостей.

Сканування вразливостей може проводитися як зовні, так і всередині мережі або сегмента мережі, що оцінюється. Організації можуть проводити зовнішнє сканування за межами периметра мережі, щоб визначити схильність до атак серверів і додатків, доступних безпосередньо з Інтернету. Тим часом, внутрішнє сканування вразливостей направлено на виявлення недоліків, які хакери можуть використовувати для переходу до різних систем і серверів, якщо вони отримають доступ до локальної мережі.

Легкість отримання доступу до частин внутрішньої мережі залежить від того, як мережа налаштована і, що більш важливо, сегментована. У зв'язку з цим будь-яка програма управління вразливостями повинна починатися зі складання карти і інвентаризації систем організації і класифікації їх важливості на основі доступу, який вони надають, і даних, які вони зберігають [15].

З широким розповсюдженням хмарної інфраструктури в останні роки, процедури сканування вразливостей повинні бути адаптовані і для хмарних активів. Зовнішнє сканування особливо важливо в цьому контексті, оскільки неправильна конфігурація і небезпечне розгортання баз даних і інших сервісів в хмарі стало звичайним явищем.

Сканування вразливостей може бути аутентифікованим і неаутентифікованим. Сканування без перевірки аутентифікації виявляє відкриті на комп'ютері служби по мережі і відправляє пакети на їх відкриті порти, щоб визначити версію операційної системи, версію програмного забезпечення, що стоїть за цими службами, наявність відкритих загальних файлових ресурсів та іншу інформацію, яка доступна без перевірки аутентифікації. На основі цих даних сканер проводить пошук в базі даних

вразливостей і встановлює список вразливостей, які, ймовірно, існують в цих системах.

Сканування з аутентифікацією використовує облікові дані для збору більш докладної і точної інформації про операційну систему і програмне забезпечення, встановлене на сканованих машинах. Деякі програми можуть бути недоступні через мережу, але все одно можуть мати вразливості, які відкривають інші вектори атак, такі як відкриття зловмисно створених файлів або відвідування шкідливих веб-сторінок.

Хоча аутентифіковане сканування збирає більше інформації і, отже, може виявити більше вразливостей, ніж неаутентифіковане, сканування вразливостей в цілому дає деякі хибні результати. Це пов'язано з тим, що можуть бути уразливості, які були усунені за допомогою різних обхідних шляхів або засобів контролю безпеки без установки файлів оновлення і оновлення версії певного додатку.

Сканування вразливостей в деяких випадках може викликати перевантаження мережі або уповільнити роботу систем, тому його часто проводять в неробочий час, коли ймовірність збоїв менше.

Вразливості, що виявлені сканерами, повинні бути розглянуті, оброблені і досліджені групами безпеки, і в багатьох випадках сканери вразливостей є частиною більш великих рішень, призначених для допомоги в процесі управління вразливостями.

Окрім, мережевих сканерів, описаних вище, існують ще сканери вразливостей веб-додатків. Сканери вразливостей веб-додатків - це спеціалізовані інструменти, що дозволяють знаходити вразливості в веб-сайтах та інших веб-додатках. У той час як мережевий сканер вразливостей сканує сам веб-сервер, включаючи його операційну систему, демон веб-сервера і різні інші відкриті служби, такі як служби баз даних, що працюють на тій же системі, сканери веб-додатків фокусуються на коді програми.

На відміну від мережевих сканерів вразливостей, які використовують базу даних відомих вразливостей і неправильних конфігурацій, сканери веб-додатків шукають такі поширені типи веб-недоліків, як міжсайтовий скриптинг (XSS), SQL

ін'єкція, ін'єкція команд і обхід шляхів. Тому вони можуть знаходити раніше невідомі вразливості, які можуть бути унікальними для тестової програми. Цей метод також відомий як динамічне тестування безпеки додатків (DAST) і часто використовується фахівцями з тестування на проникнення.

Сканери веб-додатків використовуються разом з інструментами статичного тестування безпеки додатків (SAST), які аналізують фактичний вихідний код веб-додатків на етапі розробки, як частина життєвого циклу безпечної розробки (SDLC). Залежно від того, як вони налаштовані, зовнішні засоби сканування вразливостей веб-додатків можуть генерувати великий обсяг трафіку, що може перевантажити сервер і привести до відмови в обслуговуванні і іншим проблемам. У зв'язку з цим зазвичай тестування вразливостей інтегрується в процеси DevOps і QA за допомогою так званих інтерактивних інструментів тестування безпеки додатків (IAST), які доповнюють SAST і DAST. Це допомагає виявити уразливості і небезпечні конфігурації до того, як додатки будуть запущені у виробництво.

Якщо сканування вразливостей проводиться щомісячно або щоквартально, воно дає лише моментальний знімок в часі і не відображає стан безпеки систем, що перевіряються, в період між скануваннями. Це може привести до значних прогалин, тому індустрія безпеки рекомендує збільшити частоту сканування вразливостей в рамках підходу, званого безперервним управлінням вразливостями.

2.3.2 Network traffic analysis

Системи аналізу трафіку (від англ. network traffic analysis, скороч. NTA) – системи, що виявляють загрози ІБ, досліджуючи події на рівні мережі. Вони дозволяють виявити присутність зловмисників на ранній стадії атаки, оперативно локалізувати загрози і контролювати дотримання регламентів ІБ.

Три ключові відмінності NTA-систем від інших рішень, які працюють з трафіком:

- NTA - системи аналізують трафік і на периметрі, і в інфраструктурі. Як правило, інші системи, що працюють з трафіком (IDS / IPS, міжмережеві екрани), стоять на периметрі. Тому, коли зловмисники проникають в мережу, їх дії залишаються непоміченими;
- NTA - системи виявляють атаки за допомогою комбінації способів. Машинне навчання, поведінковий аналіз, правила детектування, індикатори компрометації, ретроспективний аналіз дозволяють виявляти атаки і на ранніх стадіях, і коли зловмисник вже проник в інфраструктуру;
- застосування NTA допомагає в розслідуванні інцидентів і в threat hunting, проактивному пошуку загроз, які не виявляються традиційними засобами безпеки. NTA-системи зберігають інформацію про мережеві взаємодії, а деякі з них - ще й запис сирого трафіку. Такі дані стають корисними джерелами знань при розкручуванні ланцюжка атаки і її локалізації, а також при перевірці гіпотез в рамках threat hunting.

Виявлення атак - не єдиний сценарій застосування NTA. Такі системи допомагають розкручувати ланцюжок атаки, щоб зрозуміти хронологію її розвитку, локалізувати загрозу і прийняти компенсуючі заходи. Можна, наприклад, виявивши підозрілу спробу підключення з неавторизованого вузла на контролер домену, звернутися до історії мережевої активності вузла і перевірити, чи не було інших подібних спроб. Якщо вони траплялися, то це буде говорити про цілеспрямовані дії.

В рамках threat hunting NTA-інструментарій застосовується для перевірки гіпотез про компрометацію мережі. Наприклад, оператор системи сформулював гіпотезу, що зловмисники проникли в інфраструктуру і знаходяться на стадії горизонтального переміщення. Щоб її перевірити, він аналізує всю мережеву активність доменної інфраструктури, оскільки, щоб розвинути атаку, злочинцям потрібно провести розвідку в AD. Якщо серед підключень виявляться аномальні запити, наприклад за протоколом LDAP (протоколу доступу до каталогів), гіпотеза буде підтверджена і буде потрібно детальне розслідування.

Ще одне завдання, з яким справляються рішення класу NTA, - контроль дотримання регламентів ІБ. При розслідуванні інцидентів і під час аналізу трафіку регулярно знаходяться помилки в конфігураціях інформаційних систем і порушення корпоративних регламентів. У 9 з 10 організацій незалежно від їх розміру і сфери діяльності паролі передаються у відкритому вигляді, зустрічаються помилки конфігурації мережі, використовуються утиліти для віддаленого доступу та інструменти приховування активності. Все це серйозно збільшує шанси зловмисників на злом і розвиток атаки.

Сценарії використання NTA-систем набагато ширше в порівнянні з іншими системами, які аналізують трафік. Застосовуючи NTA, підрозділи ІБ можуть виявити атаки не тільки на периметрі, але і всередині мережі, відстежити помилки мережевої безпеки, розслідувати інциденти і полювати за загрозами. Це можливо завдяки:

- контролю як трафіку між корпоративною мережею та інтернетом, так і трафіку, що циркулює всередині організації;
- технологіям детектування загроз, специфічних для активності зловмисників всередині периметра;
- зберігання трафіку [16].

2.4 Endpoint Detection and Response system

Endpoint Detection and Response – це інтегроване рішення для забезпечення безпеки кінцевих точок, яке поєднує у собі неперервний моніторинг і збір даних про кінцеві точки в режимі реального часу з можливостями автоматизованого реагування і аналізу на основі правил.

Основними функціями системи безпеки EDR є:

- моніторинг та збір даних про активність кінцевих точок, які можуть вказувати на загрозу;
- аналіз зібраних даних для виявлення моделей загроз;

- автоматичне реагування на виявлені загрози для їх усунення чи локалізації, а також інформування співробітників команди безпеки;
- інструменти криміналістики і аналізу для вивчення виявлених загроз і пошуку підозрілої активності [17].

На рисунку 2.5 приведена стандартна схема робота EDR системи, що складається з 6 основних кроків.

Рисунок 2.5 – Схема роботи EDR системи

EDR працюють шляхом моніторингу подій кінцевих точок і мережі та запису інформації в центральну базу даних, де відбувається подальший аналіз, виявлення, розслідування, звітність і оповіщення. Програмний агент, встановлений на хост-системі, забезпечує основу для моніторингу подій і створення звітів.

Поточний моніторинг і виявлення полегшуються завдяки використанню аналітичних інструментів. Ці інструменти визначають завдання, які можуть поліпшити загальний стан безпеки компанії шляхом виявлення, реагування та відображення внутрішніх загроз і зовнішніх атак.

Не всі EDR працюють однаково або пропонують однаковий спектр можливостей. Деякі представлені на ринку програмні продукти проводять більш

глибокий аналіз на агенті, в той час як інші зосереджені на внутрішньому сервері через консоль управління. Деякі з них відрізняються за часом і масштабом збору даних або по можливості інтеграції з постачальниками даних про загрози.

Однак усі EDR системи виконують одні і ті ж основні функції з однією і тією ж метою: забезпечити засоби безперервного моніторингу та аналізу для більш швидкого виявлення, виявлення і запобігання сучасних загроз.

Більшість систем EDR вирішують задачу "реагування" за допомогою складної аналітики, яка виявляє закономірності і аномалії, такі як рідкісні процеси, дивні або нерозпізнані з'єднання або інші ризиковані дії, відмічені на основі порівняння базових показників. Цей процес можна автоматизувати, щоб аномалії викликали оповіщення для негайних дій або подальшого розслідування. Багато засобів виявлення та реагування на кінцеві точки також дозволяють проводити аналіз даних вручну або під керівництвом користувача.

Системи EDR все ще є областю, що розвивається, але можливості EDR швидко стають важливим елементом корпоративного рішення безпеки. Організаціям, які шукають саму передову систему безпеки, слід звернути увагу на можливості пропонованих EDR систем при оцінці постачальників.

Ось кілька ключових функцій EDR, на які слід звернути увагу при виборі рішення для забезпечення безпеки кінцевих точок:

Фільтрація: низькоякісні рішення, як правило, мають труднощі з фільтрацією помилкових спрацьовувань. Сповіщення включаються для подій, які насправді є загрозами, що створює втому від сповіщень і збільшує ймовірність того, що реальні загрози пройдуть непоміченими.

Розширене блокування загроз: хороше рішення буде запобігати загрозі в момент її виявлення і протягом усього життя атаки. Постійні атаки можуть в кінцевому підсумку подолати заходи безпеки на інших продуктах з більш слабким функціоналом.

Можливості реагування на інциденти: пошук загроз і реагування на інциденти можуть допомогти запобігти повномасштабному витоку даних. Наявність

рішення, яке допомагає співробітникам команди безпеки в цих зусиллях, є критично важливим для DLP.

Захист від множинних загроз: просунуті атаки або, можливо, кілька різних атак одночасно можуть вразити кінцеві точки, якщо встановлене рішення безпеки не готове до одночасного протидії декільком типів загроз (наприклад, ransomware, шкідливе ПЗ, підозрілі переміщення даних).

Для підприємств, які потребують просунутого захисту від загроз, EDR користується великим попитом. Переваги, одержувані завдяки постійній видимості всієї активності даних, роблять виявлення і реагування на кінцевих точках цінним компонентом будь-якого стеку безпеки [18].

Висновки за розділом 2

Проаналізовано причини побудови, характерні особливості, функції та методи роботи Security Operations Center. А також проаналізовано функції та переваги таких інструментальних компонентів SOC, як SIEM, сканери вразливостей, NTA та EDR.

Розглянуто основні компоненти та функції SOC на основі класифікації MITRE, а також приведено етапи побудови: формування цілей, задач та ключових параметрів SOC; визначення основних процесів та процедур SOC; дослідження інфраструктури і вибір технічних інструментів; підбір персоналу та визначення режимів роботи; навчання співробітників; контроль результатів.

Проаналізовано основний інструментальний компонент SOC – SIEM систему. При широкому представлені програмних продуктів на ринку, було виділено основні функції системи, необхідні архітектурні особливості, виявлено різноманітні випадки використання даної системи та з надано рекомендаційні висновки стосовно встановлення, використання та подальшого удосконалення системи.

Наступним інструментальним пунктом був аналіз засобів мережевої активності. Дані інструменти були розділені на два види такі, як сканери безпеки та системи NTA. Ці інструменти можна використовувати як і в комбінації та і окремо. Системи типу NTA є більш універсальними та функціональними для роботи з

мережевим трафіком, але правильне налаштування та постійний моніторинг завдяки сканерам можуть частково перекрити необхідність мережевого захисту підприємства.

Наприкінці було проаналізовано системи EDR, що виконують захист кінцевих точок. Постійний моніторинг допомагає виявити підозрілу активність, що може запобігти атакам різного типу. Однією з переваг такої системи є захист від множинних загроз, що дозволяє фокусуватися на різноманітних типах атак.

Загалом, побудова SOC є процесом тривалим. Необхідно залучати професіоналів, які правильно вибудують стратегію побудови та розвитку такого центру захисту.

РОЗДІЛ 3
РОЗРОБКА МЕТОДИЧНИХ РЕКОМЕНДАЦІЙ ТА ГРАФІЧНЕ ПРЕДСТАВЛЕННЯ РОБОТИ SOC

3.1 Методичні рекомендації для протидії APT атакам

3.1.1 Рекомендації для адміністраторів

Аби протидіяти APT атакам необхідно чітко вибудувати стратегію оборони від подібних атак. Для початку необхідно включити до стратегії оборони традиційні заходи захисту периметру і забезпечення безпеки інфраструктури. Дані заходи поділяються на два типи: організаційні та технічні заходи. Перелік рекомендованих організаційних та технічних заходів наведено на рисунку 3.1.

Рисунок 3.1 – Рекомендовані організаційні та технічні заходи для протидії APT атакам.

На рисунку 3.2 визначено, які саме етапи розгортання APT атаки блокують організаційні та технічні заходи захисту, що наведені на рисунку 3.1.

Рисунок 3.2 – Блокування розвитку APT атаки за допомогою організаційних та технічних заходів.

Щоб втілити запропоновані організаційні та технічні заходи для захисту необхідно виконати наступні кроки.

Для *розмежування повноважень та управління обліковими записами* необхідно:

- безпечно зберігати шифровані паролі співробітників підприємства;
- управляти складністю паролів (мінімальна довжина, спеціальні символи, різні регістри та регулярна зміна паролів);
- обмеження доступу до адміністративних облікових записів;

- заборона можливості автоматичної аутентифікації (веб-браузери, електронна пошта тощо);
- обмежити кількість осіб, що мають доступ до адміністративних облікових записів;
- заборона використання примітивних паролів у скриптах.

Для *мінімальних повноважень для облікових записів* необхідно реалізувати схему, за якою для виконання певних завдань користувачам необхідно шляхом авторизації чи аутентифікації отримати визначені для цього ролі, наприклад такі як системні адміністратори, адміністратори безпеки, аудитори тощо.

Для *контролю та запису сесій* необхідно:

- легка та чітка навігація у журналах запису;
- впровадження аналітичного інструментарію з метою пошуку та виявлення загроз та вразливостей (наприклад, SIEM);
- впровадити моніторинг дій користувачів.

Для *захисту серверного обладнання* необхідно:

- використовувати мережевий екран (програмний і/або апаратний), який контролює з'єднання, блокує пакети даних та небезпечні протоколи;
- впровадити політику дозволених програмних продуктів (whitelist);
- визначити критично важливе програмне забезпечення та завдання для підприємства;
- заборонити внесення змін до журналів;
- здійснювати моніторинг цілісності критично важливих файлів;
- контроль доступу до файлів та директорій.

Для *реалізації політик у нестандартних ситуаціях та при реагуванні на зовнішні загрози* необхідно:

- використовувати засоби моніторингу та захисту файлів для можливості адміністраторів виявити спроби зловмисників проникнути в мережу;
- модифікувати імена стандартних системних команд та адрес.

Для реалізації *безпеки систем та середовищ віртуалізації* необхідно:

- застосовувати принцип мінімальних повноважень та привілеїв для акаунтів гіпервізора;
- здійснювати моніторинг усіх дій, що відбуваються на рівні гіпервізора;
- автоматизувати процеси віртуалізації для підвищення захищеності віртуальних машин.

Для *управління ідентифікацією та авторизацією* необхідно:

- позбавляти повноважень в програмно-апаратних рішеннях/системах персон, які покинули підприємство;
- виконувати регулярну перевірку та видалення не актуальних облікових записів;
- реалізовувати методи багатофакторної аутентифікації;
- реалізовувати вимоги більш жорстокої аутентифікації для осіб, що мають адміністративні права.

Для *впровадження політики управління даними* необхідно:

- виконати аудит інформаційних активів підприємства, після чого визначити технології та методи захисту;
- контролювати передачу даних між підрозділами підприємства та іншими підприємства.

3.1.2 Рекомендації для користувачів

За відсутністю чітких статистичних вибірок по Україні за останні декілька років було проведено дослідження з метою визначення рівня обізнаності співробітників різноманітних підприємств щодо безпечності та коректності їх роботи з інформаційними системами. Завдяки даному дослідженню виявлено, які саме прогалини в освіті присутні у співробітників у сфері інформаційної безпеки. Кількість респондентів – 42 особи.

Опитування складалося з 29 питань, які були поділені на 5 блоків, що стосувалися роботи з електронною поштою, з'ємними носіями, інтернет браузером та дистанційної роботи і організації робочого процесу.

Найцікавіші питання наведені нижче разом з відповідями на рисунках 3.3 – 3.19.

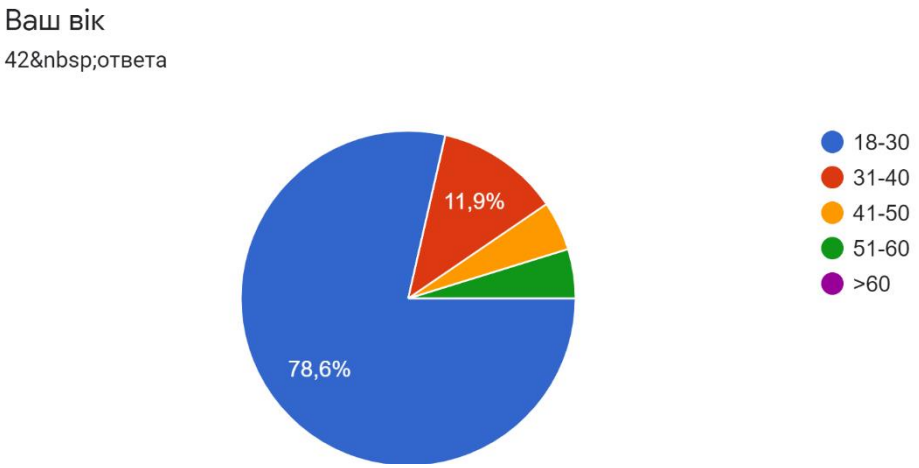

Рисунок 3.3 – Діаграма відповіді на питання

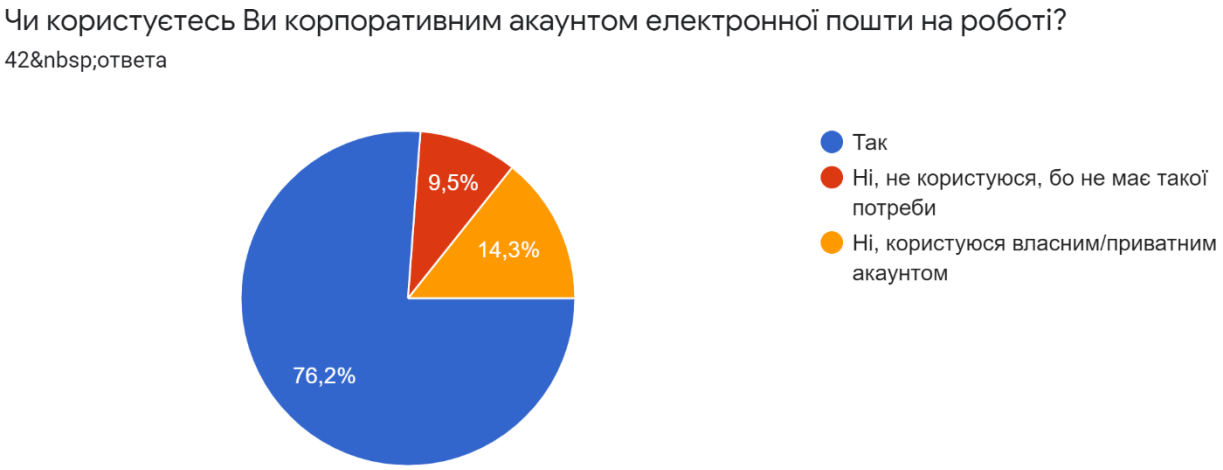

Рисунок 3.4 – Діаграма відповіді на питання

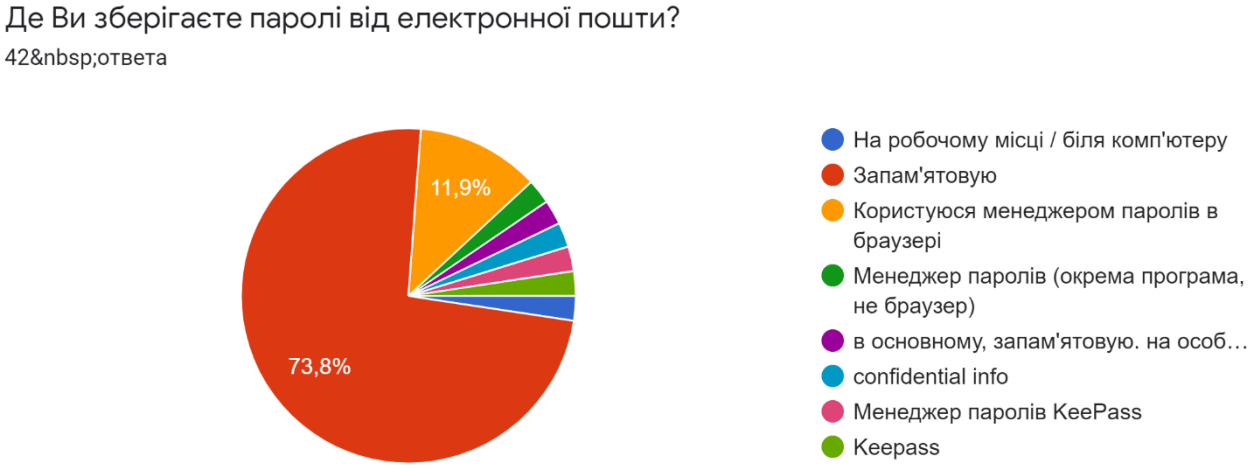

Рисунок 3.5 – Діаграма відповіді на питання

Рисунок 3.6 – Діаграма відповіді на питання

Рисунок 3.7 – Діаграма відповіді на питання

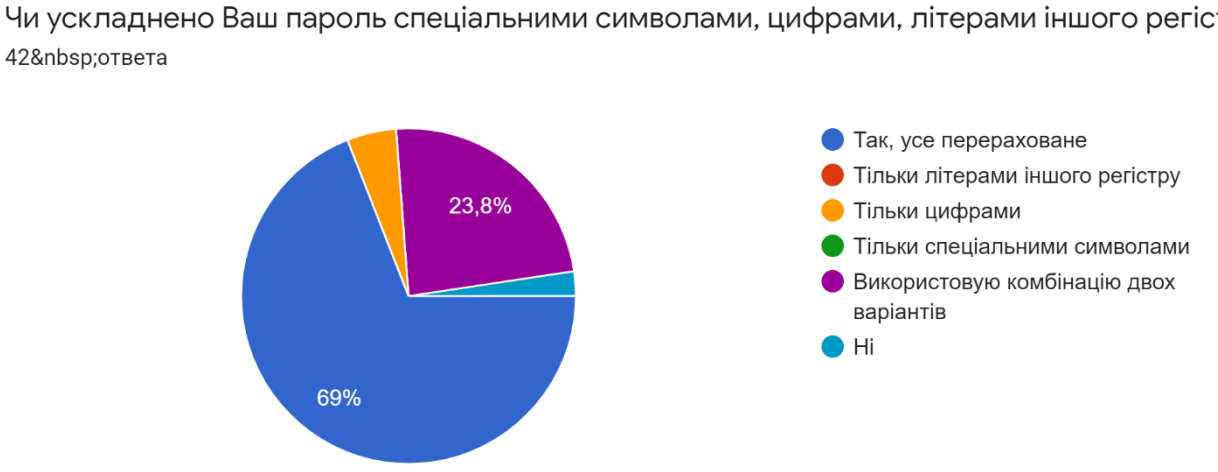

Рисунок 3.8 – Діаграма відповіді на питання

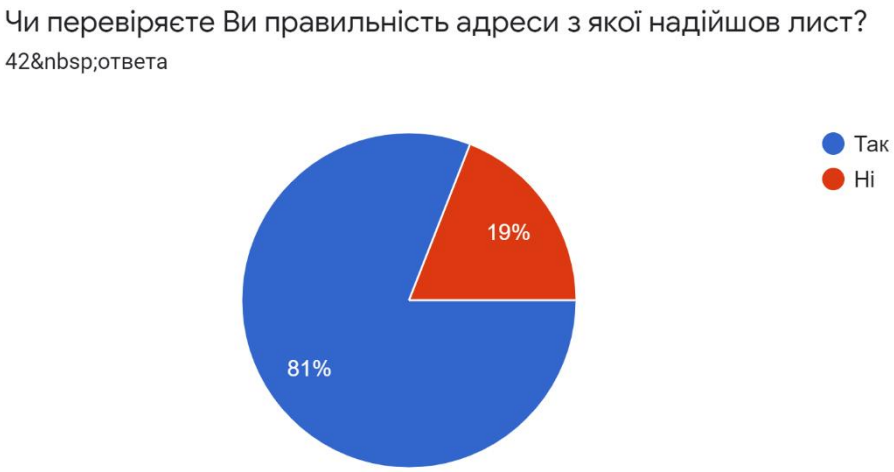

Рисунок 3.9 – Діаграма відповіді на питання

Рисунок 3.10 – Діаграма відповіді на питання

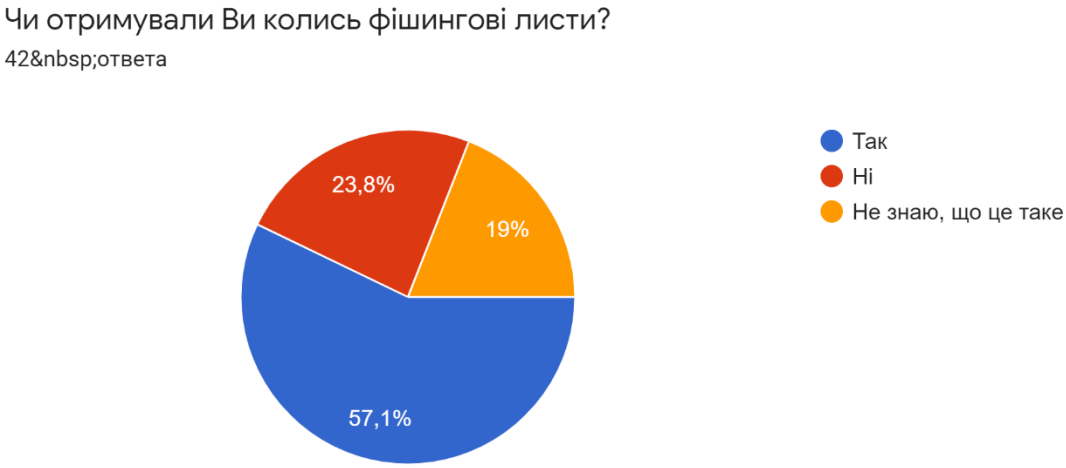

Рисунок 3.11 – Діаграма відповіді на питання

Рисунок 3.12 – Діаграма відповіді на питання

Рисунок 3.13 – Діаграма відповіді на питання

Рисунок 3.14 – Діаграма відповіді на питання

Рисунок 3.15 – Діаграма відповіді на питання

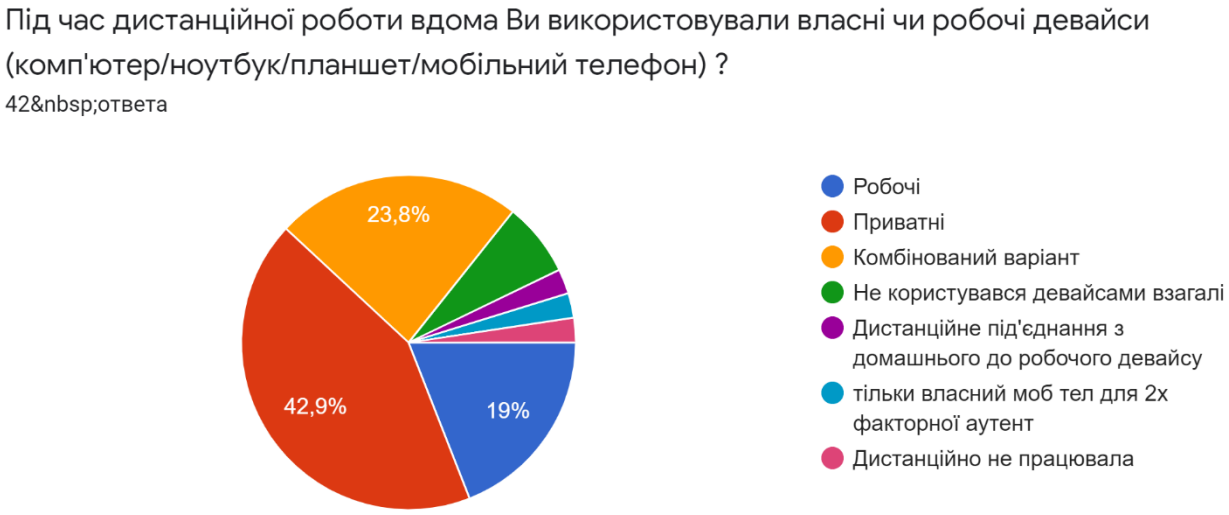

Рисунок 3.16 – Діаграма відповіді на питання

Рисунок 3.17 – Діаграма відповіді на питання

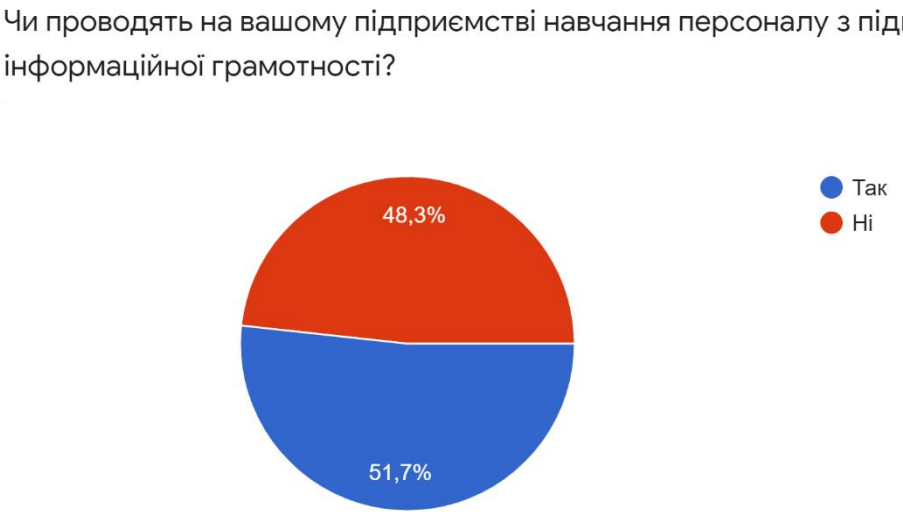

Рисунок 3.18 – Діаграма відповіді на питання

Варто зазначити, що показники з питання стосовно навчання працівників основам кібергігієни є дуже показовими. Велика кількість роботодавців ігнорують даний аспект трудової діяльності співробітників, що може призвести до серйозних матеріальних, інформаційних та репутаційних втрат.

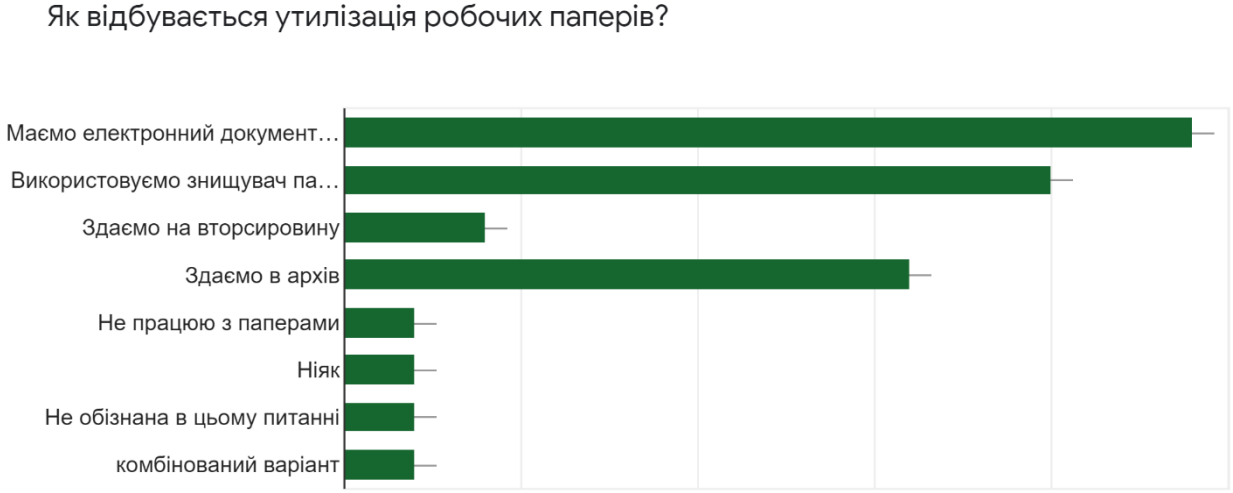

Рисунок 3.19 – Діаграма відповіді на питання

Питання стосовно утилізації паперів дало неочікувані результати. Приємно, що більшість застосовує електронний документообіг, що значно мінімізує ризики пов’язані з неправильною обробкою та/чи утилізацією службової інформації. Використання знищувача паперів та робота з архівом є також цілком безпечними варіантом. Але використання утилізація робочих паперів як за допомогою здачі як матеріал для вторинної сировини, може призвести до витоку інформації.

Зважаючи на проведене дослідження визначено області, які необхідно вивчити співробітникам для забезпечення безпечної роботи. З метою підвищення рівня обізнаності стосовно безпечної роботи варто виконувати наступні кроки.

Для мінімізації ризику зараження інформаційної системи за допомогою *електронної пошти* необхідно:

- створити акаунт корпоративної пошти, або за відсутністю корпоративного домену, створити акаунт для роботи, окремий від приватного;
- регулярно змінювати паролі від робочого поштового акаунту (хоча б раз в три місяці);
- використовувати для зберігання паролів спеціальні програмні засоби (наприклад, KeePass);
- використовувати стійкі паролі, зокрема такі що: містять не менше 8 символів; містять літери, цифри та спеціальні символи; не містять персоніфікованої інформації (дати народження, номерів телефонів, номерів та серій документів, автотранспорту, банківської картки, адреси реєстрації тощо); не використовуються в будь-яких інших аккаунтах;
- перевіряти правильність адреси з якої надійшов лист (хоча б перевірити за допомогою пошуковика);
- перевіряти вкладення та посилання, що надіслані електронною поштою, на предмет наявності шкідливого ПЗ та нелегітимного сайту (наприклад, сервісом VirusTotal).

Для мінімізації ризику зараження інформаційної системи за допомогою *інтернет браузеру* необхідно:

- під час користування Інтернет-ресурсами (Інтернет-банкінгом, соціальними мережами, системами обміну повідомленнями, новинами, онлайн-іграми) не відкривайте підозрілі посилання (URL), особливо ті, що вказують на веб-сайти, які ви зазвичай не відвідуєте;

- у разі необхідності введення аутентифікаційних даних перевірте чи використовується захищене з'єднання HTTPS (це можна зробити впевнившись у наявності «замочку» в адресному рядку браузера);
- намагайтесь уникати відвідування сайтів, що мають посилання у вигляді скороченого URL;
- намагайтесь уникати завантаження файлів з інтернет браузеру, або якщо це необхідно, то перевіряйте ці файли перед відкриттям і намагайтеся виконувати завантаження з легітимних сайтів.

Для мінімізації ризику зараження інформаційної системи за допомогою *з'ємних носіїв* необхідно:

- не під'єднувати чужі, невідомі, знайдені флешки, зовнішні диски та/або карти пам'яті до робочої станції;
- використовуйте лише власні з'ємні носії;
- при підключенні пристроїв забезпечте їх автоматичну перевірку на наявність шкідливого програмного забезпечення;
- вимкнути автоматичний запуск змінних носіїв інформації (захист від autorun.inf).

Для забезпечення безпечної *дистанційної роботи* необхідно:

- створити стійкий пароль до RDP сесій;
- якщо є можливість, варто користуватися VPN з'єднанням;
- аби уникнути зараження зі сторони приватного пристрою (якими більшість користується при дистанційній роботі) варто використовувати ліцензоване антивірусне ПЗ, яке необхідно регулярно оновлювати, увімкнути режим захисту у реальному часі;
- уникайте передачі службової інформації відкритими каналами зв'язку, якщо така можливість відсутня використовуйте шифрування.

3.2 Графічне представлення роботи SOC в інфраструктурі підприємства

Розглянемо інфраструктуру підприємства, у якій відсутні безпекові механізми, окрім антивірусного програмного забезпечення та брандмауера на кінцевих точках. Для впровадження механізмів SOC необхідно проаналізувати наявну інфраструктуру, що зображена на рисунку 3.20.

Існує дві локальні комп'ютерні мережі, по 4 кінцеві точки в кожній, які оброблюють, змінюють та зберігають критично важливу інформацію для підприємства. Дані кінцеві точки з'єднано з комутаторами та серверами баз даних, поштовими та FTP серверами. Сервери також приєднано до комутатора. Усі комутатори з'єднані з маршрутизатором, який виходить у мережу інтернет.

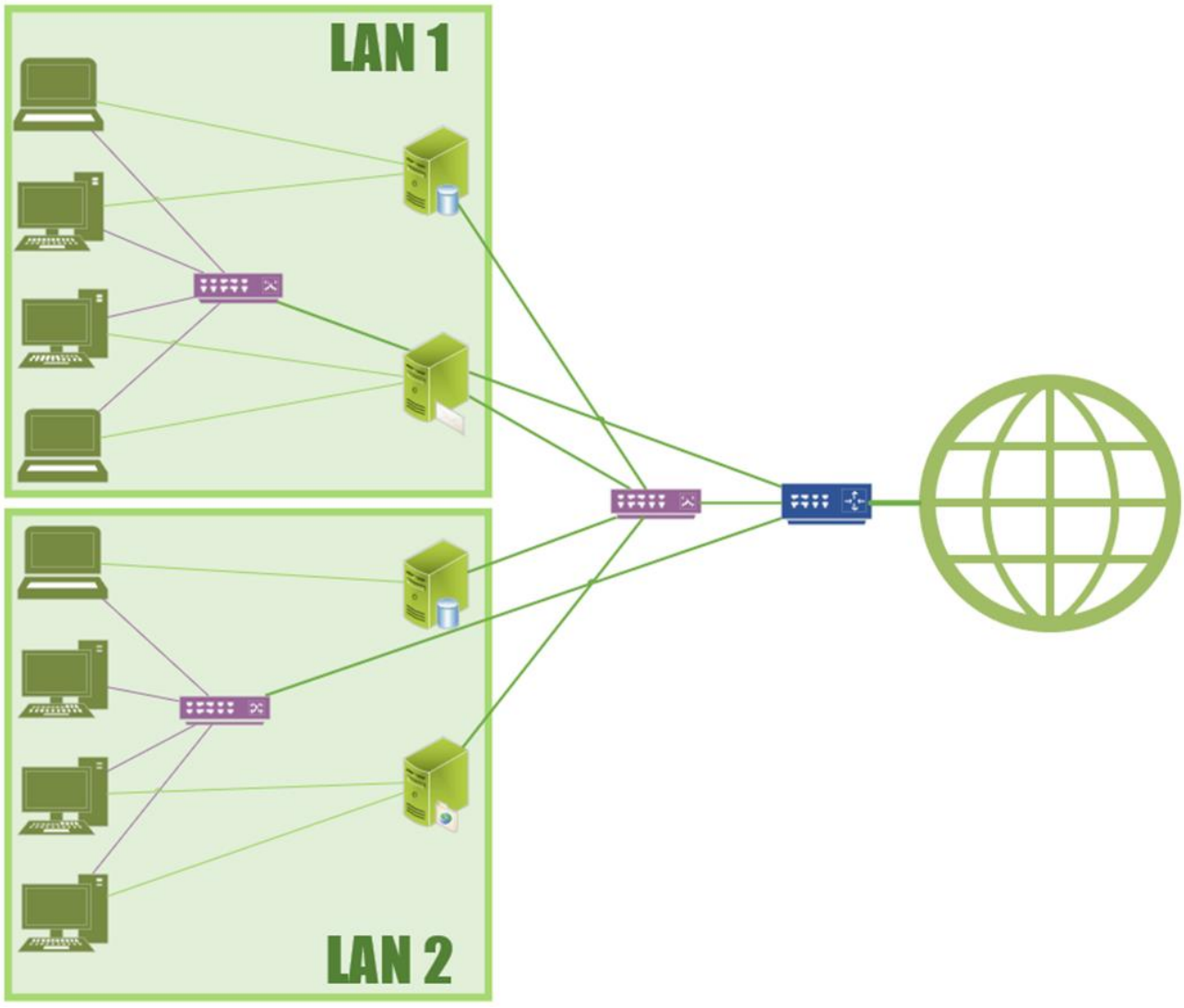

Рисунок 3.20 – Графічне зображення інфраструктури підприємства


– кінцеві точки


– FTP сервер


– комутатор


– маршрутизатор


– сервер бази даних


– мережа інтернет


– поштовий сервер

Задля впровадження SOC необхідно вдосконалити наявну інфраструктуру. Оскільки сервери баз даних не повинні мати доступ до мережі Інтернет, то необхідно провести перебудову локальної мережі 1 та 2. Кінцеві точки, що працюють з серверами баз даних, виділено в окрему локальну мережу 1. Кінцеві точки локальної мережі 1 поєднано з комутатором, який з'єднаний з маршрутизатором аби хости мали доступ до мережі Інтернет. В локальній мережі 2 знаходяться кінцеві точки, які співпрацюють з великою кількістю серверів та мають доступ до мережі Інтернет. Кінцеві точки поєднані комутатором, який з'єднано з маршрутизатором. Для більш безпечної конфігурації мережі, WEB, FTP та поштовий сервери виділено в окрему підмережу, що під'єднані до комутатора, який, в свою чергу, з'єднано з маршрутизатором для доступу в мережу Інтернет.

Окрім наявних програмних брандмауерів варто встановити апаратний між мережею інтернет та маршрутизатором. Надалі виконується під'єднання критичних точок до системи EDR, а мережевих пристроїв – до системи NTA. Після цього системи EDR та NTA підключаються до SIEM системи. Наявна «трійка» компонентів являє собою основу роботи SOC. Аналізом інформації, що надається усіма трьома система, займаються аналітики SOC. Графічне зображення вище описаного продемонстровано на рисунку 3.21.

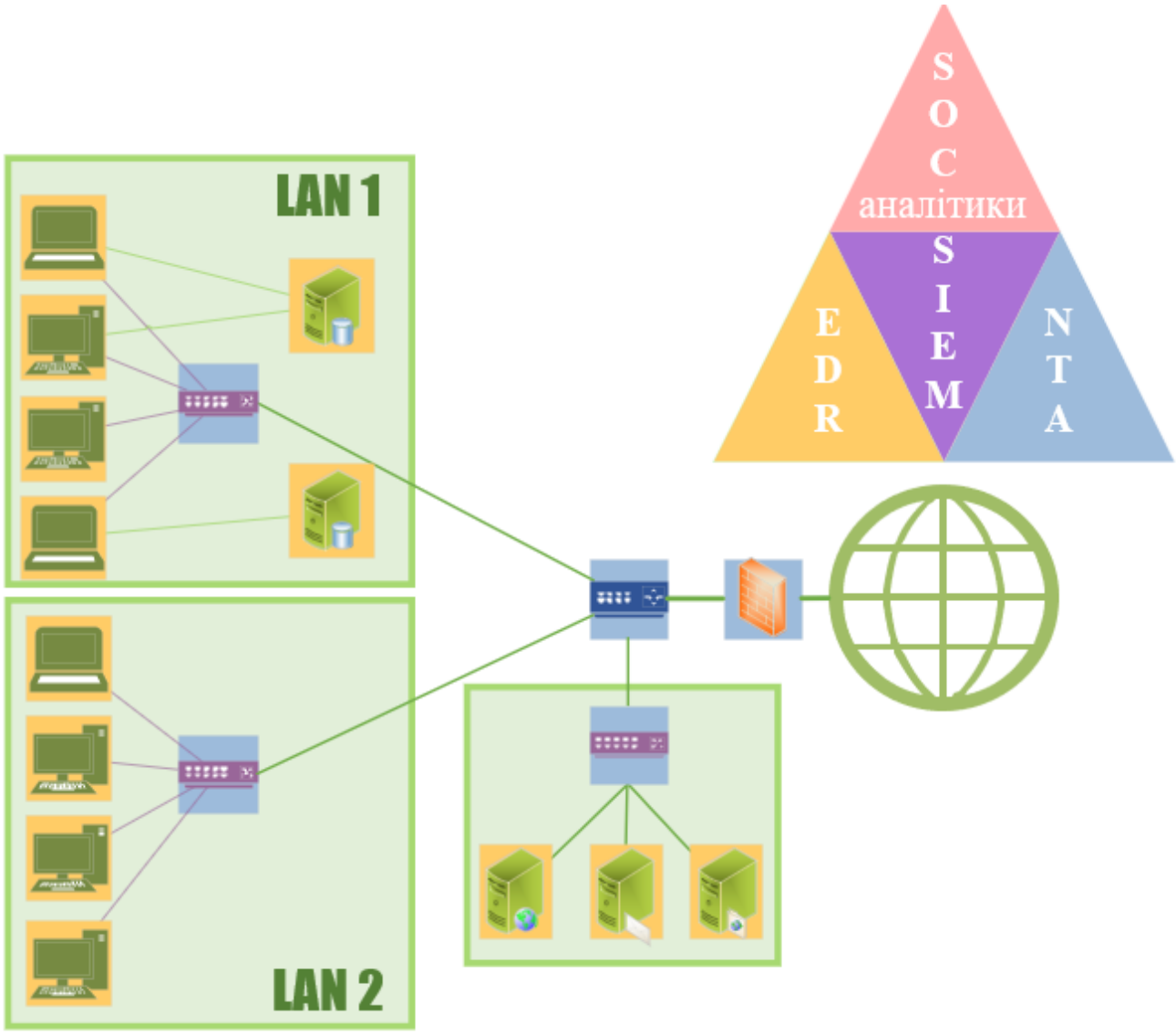

Рисунок 3.21 – Графічне зображення роботи SOC в інфраструктурі підприємства


– кінцеві точки


– комутатор


– сервер бази даних


– поштовий сервер


– FTP сервер


– WEB сервер


– маршрутизатор


– брандмауер


– мережа інтернет

3.3 Дослідження можливостей SIEM системи Splunk

SIEM система Splunk досить популярна серед адміністраторів ІБ та аналітиків завдяки простому та зрозумілому інтерфейсу і наявності великої кількості зручних механізмів для швидкого аналізу великої кількості даних.

Програмний комплекс містить такі основні вкладення як додатки (Apps), повідомлення (Messages), налаштування (Settings), активність (Activity). У вкладенні Apps містяться додатки, які допомагають користувачу в аналізі, приклад наведено на рисунку 3.22.

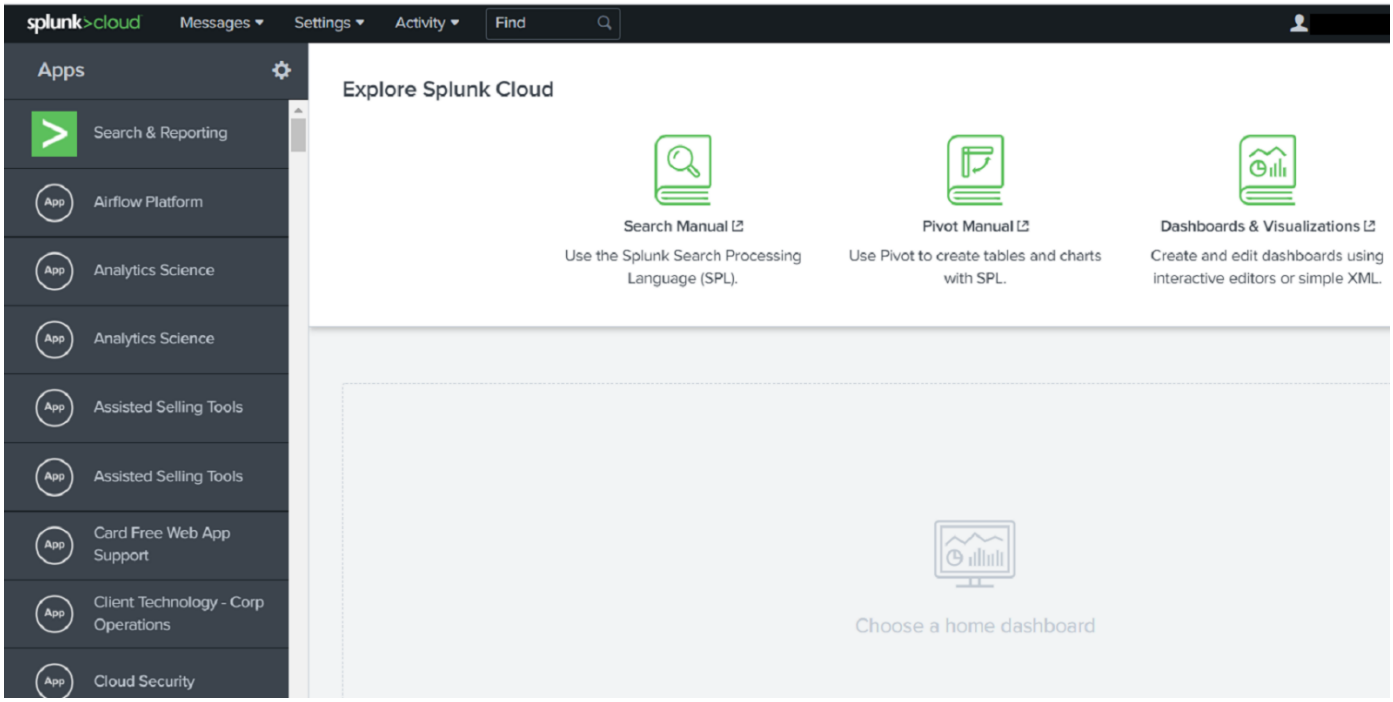

Рисунок 3.22 – Вкладення Apps в системі Splunk

Завдяки додатку Analytics Science можна використовуючи рядок пошуку фільтрувати інформацію за введеними даними та за певний період часу. Ця функція зручна при обробці великої кількості даних у режимі реального часу.

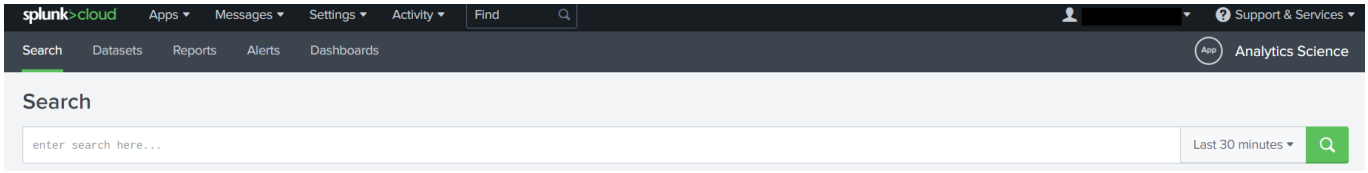

Рисунок 3.23 – Рядок пошуку в системі Splunk

Також незамінними для якісного аналізу при роботі з постійно поновлюваними даними в режимі реального часу є такі інструменти як графіки. На рисунку 3.24 відображено кількість замовлень за різноманітними статусами, зареєстрованих користувачів, запитів з різноманітних платформ, відвідування сайту та замовлення.

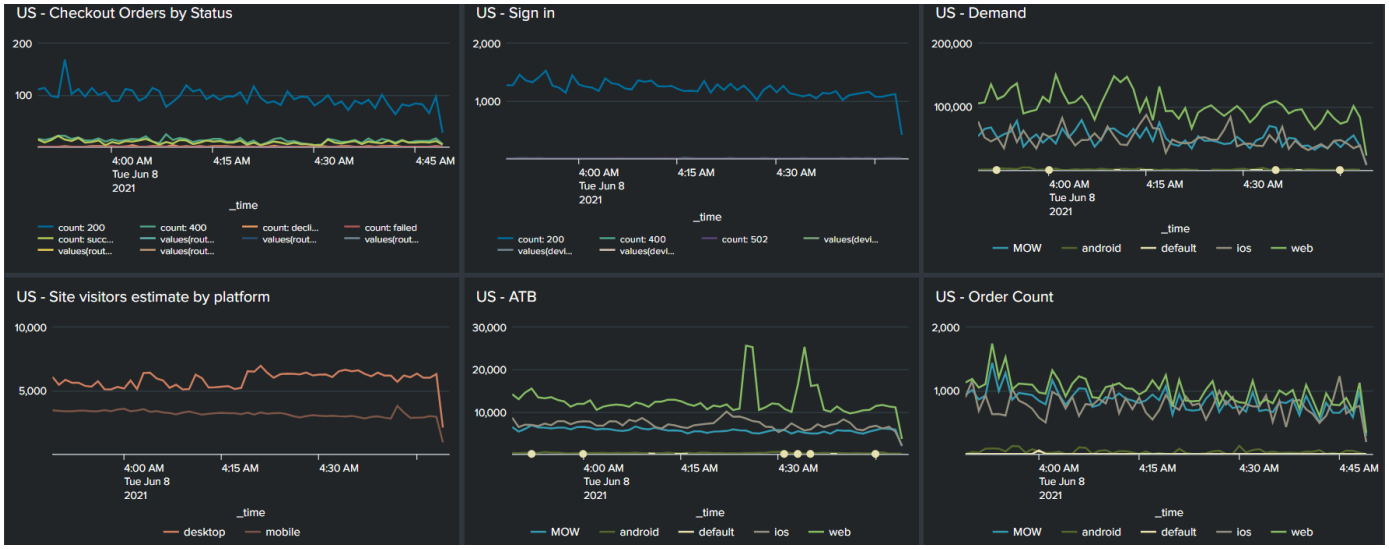

Рисунок 3.24 – Графіки вибірок в системі Splunk

Для зручності та покращення роботи можна створювати графіки за обраними показниками самостійно. На рисунку 3.25 відображено оцінка відвідувань сайту з мобільної та веб-версії, кількість замовлень за статусом, кількість запитів та замовлень, а також кількість додавання товару до «кошика» з 1 по 5 годину.

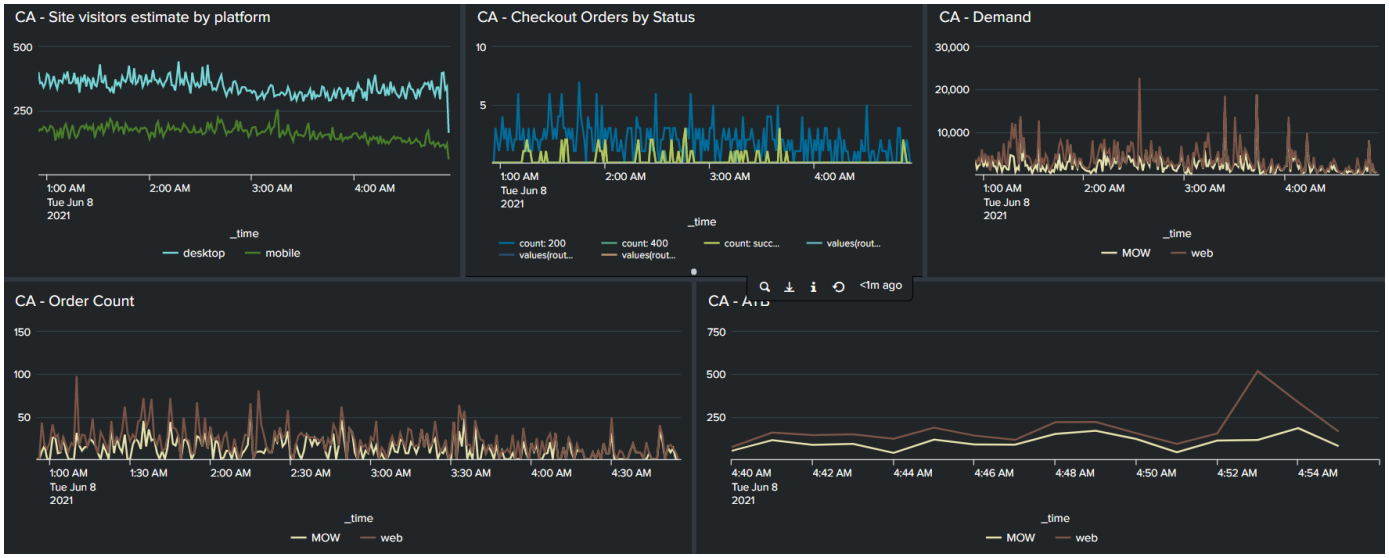

Рисунок 3.25 – Графіки вибірок в системі Splunk

Висновки за розділом 3

Розроблено рекомендації для системних адміністраторів та співробітників, а також графічне зображення роботи SOC в інфраструктурі підприємства.

Рекомендації для системних адміністраторів розроблено у комбінованому варіанті, застосовуючи передовий світовий досвід. Наведено, які саме стадії розвитку атаки блокують ті чи інші організаційні та технічні заходи захисту. А також надано інструкції з чіткими кроками, які варто виконати, аби втілити у життя масштабні захисні заходи.

Рекомендації для співробітників розроблено у зв'язку з проведеним опитуванням. Приділено увагу саме тим показникам, на яких респонденти не показали ймовірних результатів. Надані рекомендації можна застосувати для розробки тренінгу з інформаційної безпеки для співробітників підприємства.

Графічне зображення роботи SOC представлено в якості початкових етапів впровадження SOC в інфраструктуру підприємства. Визначено, які саме компоненти відносяться до EDR системи, а які до – системи NTA. Варто зазначити, що такий варіант необхідний для великого підприємства, підприємство розміром поменше може впроваджувати певні базові механізми, що значно покращить їх систему захисту без витрати значної кількості грошей.

Досліджено можливості SIEM системи Splunk за допомогою аналізу основних варіантів роботи та створено власні графіки вибірок, що дає можливість відслідковувати цікаві на даний момент події в системі та визначити наявність аномальної активності.

ВИСНОВКИ

Проаналізовано APT атаки, що є розширеною загрозою небезпечною у зв'язку з високою ймовірністю реалізації. Атаки такого типу мають декілька значних особливостей, що роблять їх складними для виявлення та протидії. Зазвичай, атака складається з 7 основних стадії. На стороні зловмисника працює високопрофесійна група, тому для адекватного захисту група професіоналів необхідна і стороні, що обороняється. Існує декілька основних типів стратегій захисту, що запропоновані ведучими світовими корпораціями в області кіберзахисту, але найкращим варіантом є комбінація запропонованих технік для побудови стратегії захисту, що необхідна певному підприємству.

З усіх запропонованих стратегій захисту вважаю, що побудова SOC на підприємстві є найбільш вдалою. Цей процес досить довготривалий, але такий варіант здатний виявити та захистити інформаційні системи від атак будь-якого рівня. Найбільш значною частиною SOC є працівники, а вже потім технічні засоби. Тому навчання не тільки співробітників SOC, а й співробітників усього підприємства являється першочерговою задачею. З технічних інструментів використовуються три основні масштабні системи – SIEM, NTA та EDR. Кожна з них відповідає за свою ділянку роботи, але без кваліфікованих аналітиків ці системи не є ефективними в повній мірі. Також, окрім цієї «трійки» варто використовувати додаткові механізми захисту, такі як сканери безпеки, впровадження методів машинного навчання та інше, що лиш підсилить обороноздатність.

У зв'язку з тим, що «людський фактор» є найбільш загрозливим у роботі з інформаційними системами було розроблено методичних вказівки для системних адміністраторів та співробітників. Проведене тестове дослідження показало, що значна частка співробітників підприємств не знають базових правил безпечного поводження з інформаційними системами. Дистанційна робота ще більше підвищила ризик вторгнення зловмисників, у зв'язку з тим, що службова інформація почала оброблюватися та зберігатися не лише на робочих пристроях. Тому

розроблені рекомендації будуть корисні для підприємств, корпорацій та державних установ аби підвищити рівень кіберграмотності співробітників.

Розробка графічного представлення роботи SOC демонструє базовий етап впровадження, коли необхідно зобразити графічно взаємозв'язок майбутніх систем. Варто зазначити, що перед цим етапом, необхідно провести аудит інформаційних активів задля визначення об'єктів, які обробляють критичну для підприємства інформацію і виконати їх підключення до систем захисту в першу чергу.

Досліджено можливості популярної SIEM системи та розроблені власні вибірки за інформацією, що збирається в режимі реального часу. Система має величезну кількість функцій та при правильному налаштуванні може значно покращити якість роботи аналітиків та допомагати у визначенні різноманітних інцидентів ІБ.

Процес захисту та протидії APT атакам є надзвичайно широкомасштабний, але необхідно розробити стратегію захисту, долучити професіоналів, які здатні втілити її в життя, впроваджувати в роботу нові засоби захисту, навчати співробітників правильному поводженню в інформаційному просторі та постійно вдосконалювати – це і є запорука ефективного захисту та стабільного робочого процесу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. В. Левцов, Н. Демидов. Анатомия таргетированной атаки. Часть 1. [Електронний ресурс]. – Режим доступу: http://samag.ru/archive/article/3170/

2. CYBER RISK REMEDIATION ANALYSIS [Електронний ресурс]. – Режим доступу: https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/cyber-risk-remediation-analysis

3. Ping Chen, Lieven Desmet, Christophe Huygens. A study on Advanced Persistent Threats. [Електронний ресурс]. – Режим доступу: https://hal.inria.fr/hal-01404186/document

4. M-Trends: the advanced persistent threat [Електронний ресурс] — Режим доступу до ресурсу: http://www.christiandve.com/wpcontent/uploads/2018/05/M-Trends.pdf

5. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains [Текст] / Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, Ph.D., — Lockheed Martin Corporation — 16 с.

6. С. Соболева. Социальная инженерия. [Електронний ресурс]. – Режим доступу: https://www.stekspb.ru/blog/it/socialnaya-inzheneriya/

7. В. Левцов, Н. Демидов. Анатомия таргетированной атаки. Часть 2. Развитие атаки. [Електронний ресурс]. – Режим доступу: http://samag.ru/archive/article/3188

8. Faisal Ali Garba. THE ANATOMY OF A CYBER ATTACK: DISSECTING THE CYBER KILL CHAIN (CKC). [Електронний ресурс]. – Режим доступу: https://journal.scsa.ge/wp-content/uploads/2019/04/3.1_5_faisal_ali_gabra2.pdf

9. Murtaza Ahmed Siddiqi, Aziz Mugher, Kanwal Oad. Advanced Persistent Threats Defense Techniques: A Review // Pakistan Journal of Computer and Information Systems Pakistan Journal of Computer and Information Systems. – 2016. – Vol.1. – No.2. – P. 53-65.

10. Алексей Воронцов. Бизнес преимущества от построения SOC на примере реальных заказчиков [Електронний ресурс]. – Режим доступу: https://www.ibm.com/ru/solutionsconnectmoscow/assets/pdf/Biznes_preimuschestva_ot_postroeniya_SOC_na_primere_realnyh_zakazchikov.pdf

11. Як швидко запустити свій Security Operation Center (SOC) [Електронний ресурс]. – Режим доступу: https://www.anti-malware.ru/analytics/Technology_Analysis/How_fast_run_SOC_Security_Operation_Center

12. What is SIEM? [Електронний ресурс]. – Режим доступу: https://www.ibm.com/topics/siem

13. Mary K. Pratt. What is SIEM software? How it works and how to choose the right tool. [Електронний ресурс]. – Режим доступу: https://www.csoonline.com/article/2124604/what-is-siem-software-how-it-works-and-how-to-choose-the-right-tool.html

14. Carson Zimmerman. Ten Strategies of a World-Class Cybersecurity Operations Center. - The MITRE Corporation, 2014. – 334 p.

15. Lucian Constantin. What are vulnerability scanners and how do they work? [Електронний ресурс]. – Режим доступу: https://www.csoonline.com/article/3537230/what-are-vulnerability-scanners-and-how-do-they-work.html

16. Что такое network traffic analysis и зачем нужны NTA-системы. [Електронний ресурс]. – Режим доступу: https://www.ptsecurity.com/ru-ru/research/knowledge-base/chto-takoe-network-traffic-analysis-i-zachem-nuzhny-nta-sistemy/

17. What Is Endpoint Detection and Response (EDR)? [Електронний ресурс]. – Режим доступу: https://www.mcafee.com/enterprise/ru-ru/security-awareness/endpoint/what-is-endpoint-detection-and-response.html

18. Nate Lord. What is Endpoint Detection and Response? A Definition of Endpoint Detection & Response. [Електронний ресурс]. – Режим доступу: https://digitalguardian.com/blog/what-endpoint-detection-and-response-definition-endpoint-detection-response

19. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. − 320 с.

20. Алексей Лукацкий. Целенаправленные атаки: из жизни невидимок / Лукацкий А. В. // !Безопасность Деловой Информации . – 2014. – №6 . – с. 4 - 9.

21. Андрей Прозоров. Как борются с APT / Прозоров А. // !Безопасность Деловой Информации . – 2014. – №6 . – с. 14 - 15.

22. Михаил Курзин. Под флагом APT / Курзин М. // !Безопасность Деловой Информации . – 2014. – №6 . – с. 16 - 18.

23. Илья Сачков. Особенности киберкриминалистики таргетированных атак / Сачков И. // !Безопасность Деловой Информации . – 2014. – №6 . – с. 38 - 40.

24. Timothy Shim. Essential Cyber Security Guide for Small Business. [Електронний ресурс]. – Режим доступу: https://www.webhostingsecretrevealed.net/blog/security/small-business-cyber-security/

25. Ellen Messmer. Gartner: 'Five Styles of Advanced Threat Defense' can protect enterprise from targeted attacks. [Електронний ресурс]. – Режим доступу: https://www.networkworld.com/article/2171375/gartner---five-styles-of-advanced-threat-defense--can-protect-enterprise-from-targe.html