МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “РОЗВІДКА ЗАГРОЗ В УПРАВЛІННІ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

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

_____ Артур Семенченко
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-42

Артур Семенченко
Ім’я, ПРІЗВИЩЕ

Керівник: Тетяна Мужанова
к.держ.упр., доцент Ім’я, ПРІЗВИЩЕ

Рецензент:
Ім’я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____ Світлана ЛЕГОМІНОВА
“____”_____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Семенченко Артуру Вікторовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Розвідка загроз в управлінні інформаційною безпекою підприємства”,
керівник кваліфікаційної роботи МУЖАНОВА Тетяна, к.держ.упр., доцент,
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджена наказом Державного університету інформаційно-комунікаційних технологійвід “27“ лютого 2024 р. № 36.

2. Строк подання кваліфікаційної роботи “20” травня 2024р.

3. Вихідні дані до кваліфікаційної роботи: *управління інформаційною безпекою підприємства, загрози інформаційній безпеці, розвідка загроз інформаційній безпеці, технології розвідки загроз інформаційній безпеці.*

4. Перелік питань, які мають бути розроблені:
4.1. Дослідити загрози інформаційній безпеці підприємства.
4.2. Встановити основні засади розвідки загроз інформаційній безпеці підприємства.
4.3. Проаналізувати практичні аспекти й розробити рекомендації щодо застосування технологій розвідки загроз на підприємстві.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “11“ березня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2024	
2.	Збір та аналіз літератури.	29.03.2024	
3.	Аналіз загроз інформаційній безпеці підприємства.	08.04.2024	
4.	Дослідження розвідки загроз в управлінні інформаційною безпекою підприємства.	22.04.2024	
5.	Вивчення практичних аспектів застосування розвідки загроз в управлінні інформаційною безпекою підприємства.	08.05.2024	
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2024	
7.	Оформлення роботи.	22.05.2024	
8.	Оформлення презентації.	03.06.2024	
9.	Отримання рецензії на роботу.	03.06.2024	
10.	Захист в ДЕК.	__.06.2024	

Здобувач вищої освіти _____ Артур СЕМЕНЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Тетяна МУЖАНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

ПОДАННЯ ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ на здобуття освітнього ступеня бакалавра

Направляється здобувач Семенченко А.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Розвідка загроз в управлінні інформаційною безпекою підприємства"

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач СЕМЕНЧЕНКО Артур у кваліфікаційній роботі дослідив загрози інформаційній безпеці підприємства; встановив основні засади розвідки загроз інформаційній безпеці підприємства, зокрема етапи життєвого циклу і джерела інформації; проаналізував практичні аспекти й розробив рекомендації щодо застосування технологій розвідки загроз на підприємстві.

СЕМЕНЧЕНКО Артур показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на Всеукраїнській науково-практичній конференції "Стратегії кіберстійкості: управління ризиками та безперервність бізнесу" 28 лютого 2024 року.

Все це дозволяє оцінити кваліфікаційну роботу здобувача СЕМЕНЧЕНКО Артура на оцінку "відмінно" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Тетяна МУЖАНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Семенченко А.В. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти СЕМЕНЧЕНКО Артура
на тему “Розвідка загроз в управлінні інформаційною безпекою підприємства”

Актуальність. Розвідка або аналіз загроз є ключовим елементом в галузі кібербезпеки, надаючи глибоке розуміння актуальних і можливих кіберзагроз. Розвідка загроз виходить за межі простого збору даних і передбачає комплексний аналіз контексту, механізмів, індикаторів, наслідків та ефективних порад щодо управління загрозами та їх суб’єктами. Таким чином, розвідка загроз є невід'ємною частиною ефективного управління інформаційною безпекою підприємства, що дозволяє вчасно виявляти і нейтралізувати потенційні загрози, забезпечуючи стабільну і безпечну роботу організації.

З огляду на зазначене дослідження значення розвідки загроз в управлінні інформаційною безпекою підприємства є актуальним науковим завданням.

Позитивні сторони.

1. У роботі досліджено основні принципи, етапи життєвого циклу й сучасні технології розвідки загроз інформаційній безпеці підприємства, представлені на ринку.

2. Оформлення кваліфікаційної роботи відповідає встановленим вимогам. Виклад матеріалу здійснено логічно й послідовно, згідно з планом, зроблено змістовні висновки. Основні положення роботи представлено у вигляді рисунків.

3. Автор опрацював значну джерельну базу, переважно англомовну, зокрема дані статистики про загрози інформаційній безпеці, описи програмних рішень розвідки загроз від виробників.

4. За результатами дослідження розроблено практичні рекомендації щодо застосування технологій розвідки загроз інформаційній безпеці на підприємстві.

Недоліки.

Доцільно було б приділити більше уваги вивченню ролі розвідки загроз у системі управління інформаційною безпекою підприємства, порівнянню технологій розвідки загроз.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “відмінно”, а здобувач СЕМЕНЧЕНКО Артур заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент:

_____
підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню засад розвідки загроз в управлінні інформаційною безпекою підприємства. Робота складається зі вступу, трьох розділів, що містять 21 рисунок, висновків і списку використаних джерел із 45 найменувань. Загальний обсяг роботи становить 78 аркушів, з яких 6 аркушів займають перелік умовних скорочень і список використаних джерел.

Метою роботи є дослідження значення розвідки загроз в управлінні інформаційною безпекою підприємства.

Об'єктом дослідження є управління інформаційною безпекою підприємства.

Предмет дослідження – розвідка загроз в управлінні інформаційною безпекою підприємства.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу, класифікації та порівняння, прогнозування й оцінки загроз і ризиків, функціонального аналізу засобів виявлення загроз.

Як результат у роботі досліджено загрози інформаційній безпеці підприємства; встановлено основні засади розвідки загроз інформаційній безпеці підприємства; проаналізовано практичні аспекти й розроблено відповідні рекомендації щодо застосування технологій розвідки загроз на підприємстві.

Галузь застосування. Розроблені підходи можуть бути використані в управлінні інформаційною безпекою підприємства для підвищення ефективності процесів аналізу й виявлення актуальних і потенційних інформаційних та кіберзагроз.

Ключові слова: УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА, ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ, РОЗВІДКА ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ, ТЕХНОЛОГІЇ РОЗВІДКИ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ.

ABSTRACT

The qualification work is devoted to the study of threat intelligence principles in the information security management of an enterprise. The work consists of an introduction, three chapters containing 21 figures, conclusions and a list of 45 references. The total volume of the work is 78 pages, of which 6 pages are occupied by a list of abbreviations and a list of references.

The purpose of the study is to investigate the principles of information security awareness and training for personnel.

The object the study is enterprise information security management.

The subject of the study is threat intelligence in the management of enterprise information security.

Research methods. To solve the above-mentioned scientific task, the methods of analysis, classification and comparison, forecasting and assessment of threats and risks, functional analysis of threat detection tools are used in the work.

As a result, the paper investigates threats to the information security of the enterprise; establishes the basic principles of intelligence of threats to the information security of the enterprise; analyzes practical aspects and develops appropriate recommendations for the use of threat intelligence technologies in the enterprise.

Field of application. The developed approaches can be used in the information security management of the enterprise to increase the efficiency of the processes of analysis and detection of actual and potential information and cyber threats.

Keywords: ENTERPRISE INFORMATION SECURITY MANAGEMENT, INFORMATION SECURITY THREATS, INFORMATION SECURITY THREAT INTELLIGENCE, INFORMATION SECURITY THREAT INTELLIGENCE TECHNOLOGIES.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

AIT	Automated Information Technology
APT	Advanced Persistent Threat
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CTI	Cyber Threat Intelligence
CVE	Common Vulnerabilities and Exposures
CVRF	Common Vulnerability Reporting Framework
CWE	Common Weakness Enumeration
DNS	Domain Name System
DoS/DDoS	Denial-Of-Service/(Distributed) Denial-Of-Service
EDR	Endpoint Detection and Response
ICMP	Internet Control Message Protocol
IoC	Indicators of Compromise
MFA	Multifactor Authentication
MitM	Man-in-the-Middle
NIDS	Network Intrusion Detection System
OWASP	Open Web Application Security Project
OSINT	Open Source Intelligence
RMON	Remote MONitoring
SIEM	Security Information and Event Management
SOAR	Security Orchestration Automation and Response
SOC	Security Operation Center
TIP	Threat Intelligence Platform
TTPs	Tactics, Techniques, and Procedures
WAF	Web Application Firewall
WEF	Windows Event Forwarding

ВСТУП

Актуальність теми. Розвідка загроз в інформаційній безпеці підприємства є важливим аспектом сучасного управління інформаційною безпекою. Розвідка загроз є ключовим елементом інформаційної безпеки підприємства, оскільки вона дозволяє: прогнозувати потенційні атаки, адаптувати захисні механізми, зменшувати ризики, підвищувати обізнаність персоналу та забезпечувати відповідність нормативам. Таким чином, розвідка загроз є важливою для забезпечення стійкості інформаційних систем підприємства та захисту від сучасних інформаційних та кіберзагроз.

З огляду на зазначене дослідження значення розвідки загроз в управлінні інформаційною безпекою підприємства є актуальним науковим завданням.

Мета роботи полягає у дослідженні значення розвідки загроз в управлінні інформаційною безпекою підприємства.

Об'єкт дослідження – управління інформаційною безпекою підприємства.

Предмет дослідження – розвідки загроз в управлінні інформаційною безпекою підприємства.

Для досягнення цієї мети в роботі необхідно виконати такі **завдання**:

1. Дослідити загрози інформаційній безпеці підприємства.

2. Встановити основні засади розвідки загроз інформаційній безпеці підприємства.

3. Проаналізувати практичні аспекти застосування технологій розвідки загроз на підприємстві, розробити практичні рекомендації.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та оцінки загроз та ризиків, моніторингу безпеки, інформаційної розвідки, життєвого циклу та інструментів для розвідки та усунення загроз.

Практичне значення одержаних результатів. Впровадження розробки дозволить зробити обґрунтований вибір методів та інструментів для аналізу

загроз у інформаційній безпеці та стане ключовим елементом управління інформаційною безпекою відповідно до бізнес-цілей, можливостей та ресурсів підприємства.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 28 лютого 2024 року.

Розділ 1 ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА

1.1 Основи управління інформаційною безпекою

Інформаційна безпека є основоположним елементом діяльності будь-якої організації, установи і підприємства, а також важливою складовою поведінки людини. Розуміння основ інформаційної безпеки допоможе організаціям і громадянам захистити себе, партнерів, клієнтів і близьких людей від негативних наслідків реалізації інформаційних загроз.

Під інформаційною безпекою будемо розуміти захищеність інформації й інфраструктури, яка її підтримує від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати неприйнятної шкоди суб'єктам інформаційних відносин, у тому числі власникам і користувачам інформації й підтримуючої інфраструктури [1].

Інформаційна безпека має чотири основні принципи (Рис. 1.1): конфіденційність, цілісність, доступність і неспростовність:

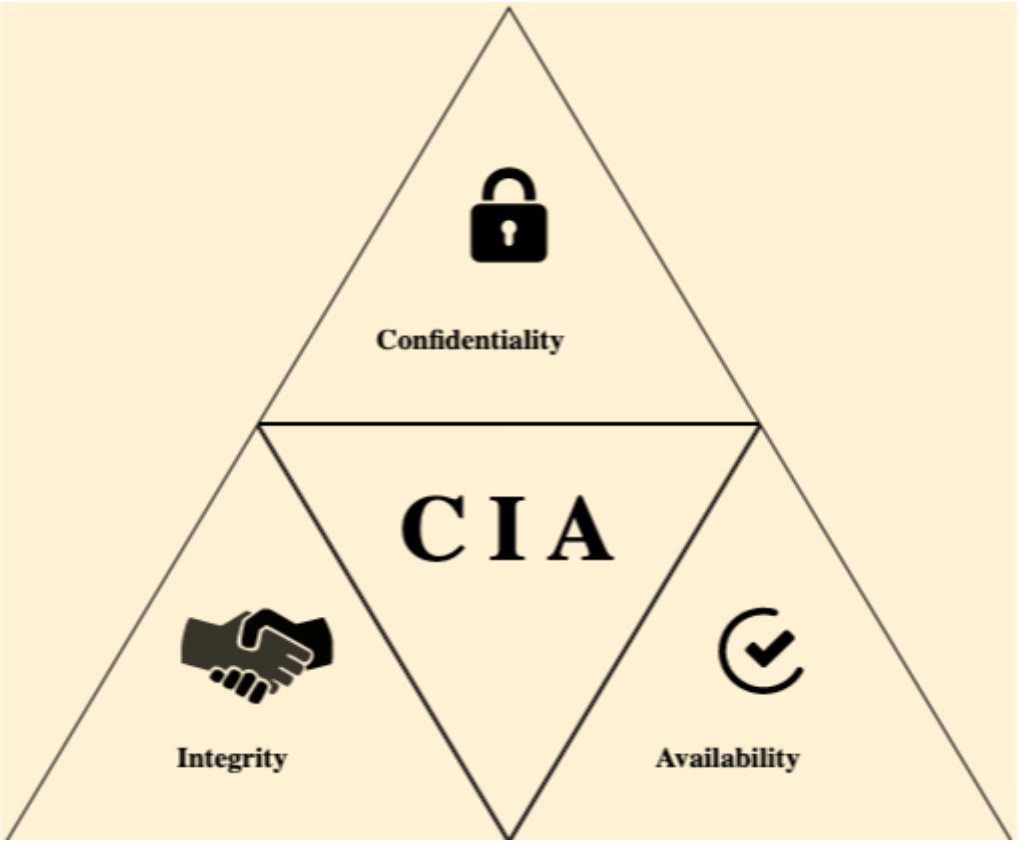

Рис. 1.1. Основні принципи інформаційної безпеки.

Конфіденційність передбачає, що лише уповноважені особи мають доступ до певної інформації.

Цілісність означає, що дані не можуть бути змінені без дозволу.

Доступність гарантує, що авторизовані користувачі можуть отримати доступ до необхідних їм даних, коли їм це потрібно.

Неспростовність (неможливість відмовитися від відповідальності або вчинення певних дій в системі) означає, що ніхто не може заперечувати, що він вчинив якусь дію, наприклад, надіслав електронного листа.

Забезпечення конфіденційності має на меті захист конфіденційних даних від неавторизованих осіб і може охоплювати шифрування даних під час їхнього зберігання або передачі, впровадження засобів і заходів контролю доступу, щоб тільки авторизовані користувачі могли переглядати або змінювати дані.

Забезпечення цілісності передбачає запобігання можливості неавторизованих осіб навмисно або випадково підробити дані, і, як результат гарантувати повноту і точність інформації.

Заходи щодо забезпечення доступності охоплює, зокрема діяльність щодо резервного копіювання й аварійного відновлення даних у разі серйозного збою [2].

Кібербезпека є складовою інформаційної безпеки й охоплює захист інформації в цифровій формі, а також засобів її обробки і передачі від інформаційних загроз, які походять переважно з мережі Інтернет.

На думку фахівців IBM, кібербезпека стосується будь-яких технологій, заходів і видів діяльності з метою запобігання кібератакам або пом’якшення їхніх наслідків [3].

Відповідно до бачення CISCO кібербезпека є діяльністю щодо захисту систем, мереж і програм від цифрових атак [4] IT Governance до об’єктів захисту від кібератак крім систем, мереж і програм додає ще пристрої і дані [5].

У контексті захисту особи від кібератак кібербезпека передбачає захист особистих пристроїв і облікових записів в Інтернеті від несанкціонованого доступу та крадіжки. Це охоплює забезпечення надійності й унікальності

паролів, використання двофакторної автентифікації, де це можливо, й обережне ставлення до посилань і вкладень, на які може натиснути користувач мережі.

Кібербезпека набуває щораз більшого значення зі зростанням кількості і складності кіберзагроз, які можуть призвести до витоку конфіденційних даних, фінансових втрат і навіть фізичної шкоди, а кіберзлочинність стає однією з найсерйозніших загроз, з якими стикаються компанії і приватні особи.

Тим не менше, низка простих заходів можуть забезпечити захист від кібератак, зокрема оновлення програмного забезпечення й операційної системи, використання надійних паролів і уважне ставлення до посилань і вкладень, на які ви натискаєте. Дотримуючись цих простих порад, ви зможете захистити себе від зростаючої загрози кіберзлочинності.

Відповідно до концепції Міжнародної організації зі стандартизації ISO, розробника серії стандартів ISO 27000 управління інформаційною безпекою передбачає розроблення, впровадження, функціонування, моніторинг, перегляд, підтримку і вдосконалення інформаційної безпеки організації [6].

Ефективне управління інформаційною безпекою реалізується згідно з такими принципами:

- комплексність (всеосяжність, охоплення заходами безпеки всіх компонентів ІС і врахування всіх актуальних і потенційних факторів ризику);
- узгодженість з бізнес-завданнями і стратегією розвитку компанії;
- високий рівень керованості й адаптивності до динамічних умов оточення;
- повнота, актуальність, достовірність інформації, яка використовується в управлінні;
- дотримання балансу між можливостями, продуктивністю і витратами на безпеку;
- безперервність управлінського впливу;
- поєднання процесів управління в замкнутий цикл «Планування – впровадження – перевірка – удосконалення» [7].

У рамках комплексного підходу для управління інформаційною безпекою організації чи підприємства здійснюють комплекс заходів, які полягають у

захисті інформаційних систем і даних від несанкціонованих доступу, використання, розкриття, втручання, модифікації та знищення. Заходи інформаційної безпеки можна розділити на три великі категорії: адміністративні, фізичні й технічні (Рис. 1.2).

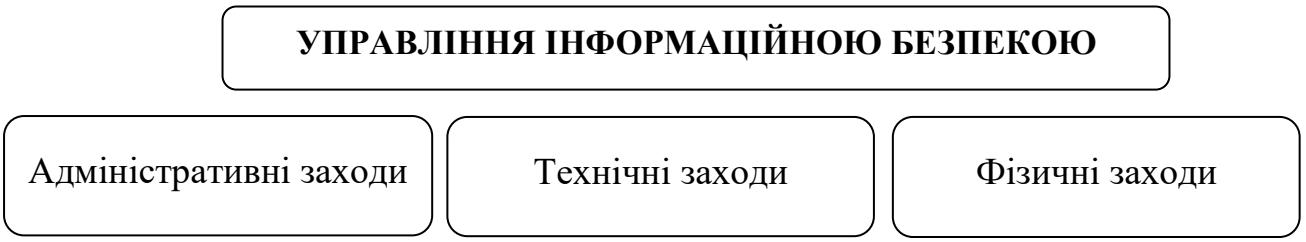

Рис. 1.2. Заходи управління інформаційною безпекою організації

Адміністративні заходи - це процедури й політики, які допомагають захистити інформаційні системи та дані. Вони охоплюють:

1. класифікацію активів;
2. визначення прав доступу до систем і даних;
3. встановлення рівнів допуску до систем і даних;
4. розподіл обов'язків із управління інформаційною безпекою;
5. розроблення програм підвищення обізнаності та навчання з безпеки;
6. оцінювання ризиків;
7. розроблення плану реагування на інциденти тощо.

Фізичні заходи призначені для захисту інформаційних систем і даних від фізичних загроз, таких як пожежа, повінь, вимкнення електроенергії, різкі перепади температури, злом і крадіжка. Приклади фізичних заходів включають використання фізичних пристроїв безпеки, таких як замки і сигналізація, а також установку засобів контролю навколишнього середовища.

Технічні заходи мають на меті захистити інформаційні системи та дані від логічних або кіберзагроз. До них належать такі заходи як установка брандмауерів і систем виявлення вторгнень, створення облікових записів користувачів і паролів, шифрування даних, впровадження списків контролю доступу, аудит діяльності системи тощо [7].

Основні компоненти управління інформаційною безпекою охоплюють (Рис. 1.3):

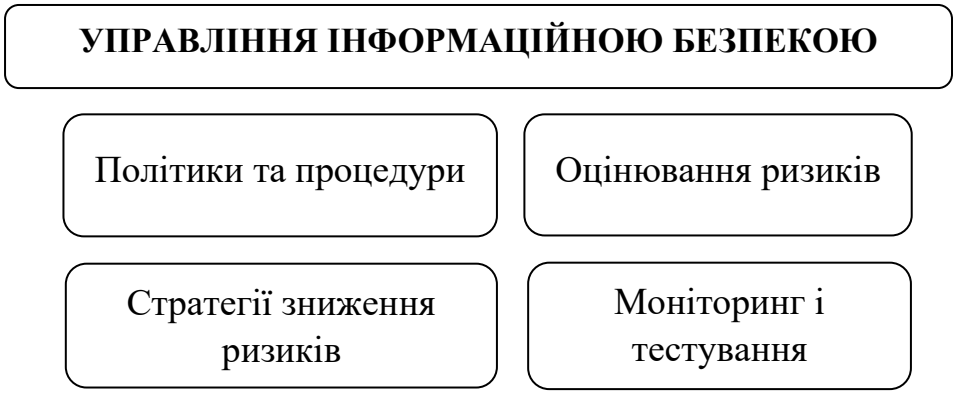

Рис. 1.3. Основні компоненти управління інформаційною безпекою

Політики та процедури: організації необхідно розробити чіткі політики і процедури для захисту конфіденційних даних, які мають регулярно переглядатися й оновлюватися з урахуванням змін у бізнес-середовищі й технологіях.

Оцінювання ризиків: оцінювання ризиків має проводитися на регулярній основі для виявлення потенційних загроз і вразливостей. Під час оцінювання слід враховувати тип даних, їхню чутливість і потенційні наслідки порушення безпеки.

Стратегії зниження ризиків: після виявлення ризиків необхідно впровадити стратегії зниження ризиків, щоб зменшити ймовірність або наслідки інцидентів. До них належать технічні заходи (брандмауери та системи виявлення вторгнень, а також організаційні заходи, як-от навчання співробітників.

Моніторинг і тестування: інформаційну безпеку потрібно постійно контролювати, щоб переконатися в тому, що в організації дотримуються політик і процедур безпеки, а заходи управління є ефективними. Необхідно регулярно проводити тестування для виявлення слабких місць і вразливостей системи управління інформаційною безпекою [7].

1.2 Загрози інформаційній безпеці: джерела й тенденції розвитку

Усі компанії, від малих і середніх до великих, потребують захисту своїх даних. Крім інформації, захисту підлягає комп'ютерне обладнання й усі технічні

засоби, які контактують з цінною інформацією. У зв'язку з тим, що інформація в руках злочинців є небезпечною, організації необхідно докласти максимум зусиль для забезпечення достатнього рівня захищеності інформаційних систем, який необхідно постійно вдосконалювати і посилювати, з метою запобігання і протидії хакерам і злочинцям, що весь час вдосконалюють свої методи злому та проникнення.

Загрози інформаційній безпеці - це дії або події, які потенційно можуть порушити конфіденційність, цілісність або доступність даних чи систем. Інформаційні загрози можуть походити з різних джерел, зокрема від окремих осіб, груп, технічних пристроїв, програм або природних явищ [8].

Джерела загроз інформаційній безпеці

Говорячи про загрози інформаційній та кібербезпеці, важливо розуміти, хто є їх суб'єктами і які тактики, технології і процедури (ТТП) вони використовують. До поширених джерел інформаційних та кіберзагроз належать (Рис. 1.4):

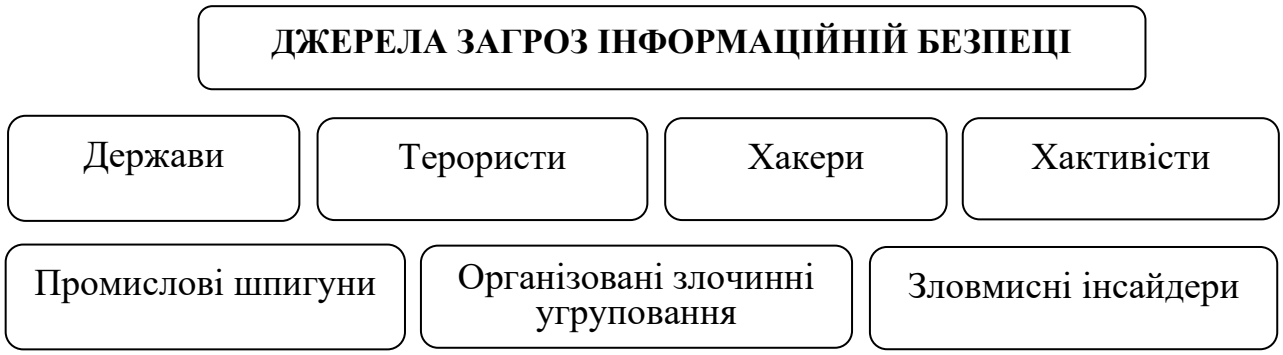

Рис. 1.4. Основні джерела загроз інформаційній безпеці

Держави - кібератаки з боку держав можуть порушити комунікації, військову діяльність або інші послуги, якими громадяни постійно користуються.

Терористи можуть атакувати урядові або військові об'єкти, або іноді також націлюватися на цивільні веб-сайти, щоб вивести їх з ладу і завдати довготривалої шкоди.

Промислові шпигуни здійснюють незаконне добування відомостей, що становлять комерційну цінність, зокрема про тактичні та стратегічні наміри

бізнесу, корпоративні ноу-хау, на замовлення конкурентів з метою отримання фінансової вигоди.

Організовані злочинні угруповання проникають і зламують системи з метою отримання грошової вигоди. Організована злочинність використовує фішинг, спам і шкідливе програмне забезпечення для крадіжки особистих даних і різноманітних шахрайств в Інтернеті. Існують організовані злочинні групи, які продають хакерські послуги, надаючи підтримку й послуги як спекулянтам, так і промисловим шпигунам.

Хакери - у світі існує велика популяція хакерів, починаючи від початківців-«скриптових дітлахів» або тих, хто використовує готові набори інструментів для створення загроз, і закінчуючи досвідченими операторами, які можуть розробляти нові типи загроз і уникати організаційних засобів захисту.

Хактивісти - це хакери, які проникають або порушують роботу систем з політичних чи ідеологічних причин, а не заради фінансової вигоди.

Зловмисні інсайдери становлять дуже серйозну загрозу, оскільки вони мають доступ до корпоративних систем і знання про об’єкти та конфіденційні дані, які є цілями кібератак. Інсайдерські загрози можуть бути руйнівними і їх дуже важко виявити [8].

Тенденції розвитку загроз ІБ

Цифрова епоха докорінно змінила спосіб ведення бізнесу, оскільки Інтернет та інформаційно-комунікаційні технології відіграють центральну роль у функціонуванні сучасного бізнесу. Але разом з цим прогресом з'являється ризик кібератак і витоку даних, які ставлять під загрозу підприємства та їхніх клієнтів. Оскільки кіберзагрози продовжують розвиватися і стають все більш витонченими, життєво важливо, щоб бізнес мав надійні заходи інформаційної та кібербезпеки, щоб захистити себе від атак.

Згідно з дослідженням компанії Proofpoint, що спеціалізується на кібербезпеці, опитані у 2023 році 1600 керівники служб інформаційної безпеки (CISO) по всьому світу визнають, що їхні організації схильні до ризику значних кібератак у найближчій перспективі [9].

Так, 68% респондентів вважають, що їхня організація зазнає атаки в наступні 12 місяців, з них 25 % оцінюють імовірність цього як дуже високу. Для порівняння: у попередньому році тільки 48 % вважали, що в найближчі 12 місяців їхні організації зазнають кібератаки.

Майже дві третини CISO вже мали справу з втратою конфіденційних даних за попередні 12 місяців. Географічно найбільш стурбованими внаслідок загроз безпеці є CISO у Великобританії (84%), Німеччині (83%) і Сінгапурі (80%), а в США – 73%. Що стосується бізнес-напрямів, то найбільше занепокоєння щодо кібератак відчувають CISO у роздрібній торгівлі (77%), виробництві (76%) та фінансах (71%).

Також дослідження визначило такі основні тенденції розвитку галузі інформаційної та кібербезпеки [8] (Рис. 1.5.).

Рис. 1.5. Тенденції розвитку галузі інформаційної та кібербезпеки

Кількість зловмисних атак зростає

Зловмисники завжди становили серйозну загрозу для бізнесу. Однак зі стрімким розвитком технологій в останні роки кібератаки стали частішими та витонченішими, ніж будь-коли раніше. За останніми даними, атака відбувається кожні 39 секунд. Це один з показників кібербезпеки, який викликає велике занепокоєння кожного підприємця.

Витоки даних коштують дуже дорого

Будь-який тип витоку даних дуже дорого обходиться бізнесу з точки зору втраченого часу, ресурсів і доходів. За результатами дослідження, до 2025 року кібератаки коштуватимуть бізнесу 10,5 трильйонів доларів США на рік. Ці гроші можна було б використати для стимулювання інновацій, створення робочих місць і побудови більш безпечного майбутнього як для бізнесу, так і для клієнтів.

Фішинг становить серйозну загрозу

Кіберзлочинці мають необмежену кількість способів проникнення в системи компаній. Однак одним з їхніх улюблених методів є фішинг. Фішинг - це надсилання електронних листів, які виглядають як легітимні джерела інформації, але побудовані таким чином, щоб виманити конфіденційну інформацію, таку як паролі або реквізити банківських рахунків.

Насправді, 90% витоків даних відбуваються в результаті фішингових атак. Якщо організації хочуть залишатися захищеними, важливо бути уважними до спроб фішингу та вживати заходів для мінімізації ризиків [10].

Більшість порушень безпеки спричинені людськими помилками

У більшості організацій відповідальність за безпеку несуть насамперед фахівці із захисту інформації. Однак людські помилки, випадкові чи зловмисні, також можуть призвести до витоку інформації. Так, 95% витоків даних спричинені саме людськими помилками, які варіюються від натискання на незахищені посилання до шахрайства з електронною поштою.

Навчання з кібербезпеки має важливе значення

Якщо людська помилка є основною причиною витоку даних, то навчання персоналу з безпеки є одним з найефективніших інструментів у боротьбі з

кібератаками. Згідно з опитуванням, 97% респондентів заявили, що пройшли тренінг з кібербезпеки протягом минулого року. Навчання працівників щодо того, як виявляти й запобігати таким атакам, як фішинг і шкідливе програмне забезпечення, може допомогти організації залишатися в безпеці.

Витрати на IT-безпеку зростають

Зловмисники постійно вдосконалюють свої навички і знаходять нові способи проникнення в системи. Це є викликом для бізнесу, який вимагає інвестицій у вдосконалений кіберзахист, як ніколи раніше. Так, витрати на IT-безпеку перебувають на рекордно високому рівні і до кінця 2022 року перевищать 172 мільярди доларів США.

Значне зростання використання пристроїв Інтернету речей

Однією з найсерйозніших загроз кібербезпеці, з якими сьогодні стикається бізнес, є зростаюче використання пристроїв Інтернету речей. Якщо пристрої Інтернету речей не захищені належним чином, зловмисники можуть легко отримати доступ до мережі компанії через них. Однак, зважаючи на те, що до 2025 року очікується використання понад 75 мільярдів пристроїв Інтернету речей, організаціям вкрай важливо вжити заходів для забезпечення максимальної безпеки цих пристроїв.

Зростаючий дефіцит персоналу з IT-безпеки

Персонал з IT-безпеки є важливим ресурсом у боротьбі з кібератаками. Оскільки потреба в цих фахівцях зростає, розрив між попитом і пропозицією збільшується. За оцінками фахівців, до 2021 року близько 3,5 мільйона вакансій залишаться незаповненими у всьому світі, а в найближчі роки цей розрив лише зростатиме.

Більшість компаній не мають плану реагування на інциденти кібербезпеки

Незважаючи на велику кількість кібератак, 77% організацій у всьому світі все ще не мають ефективного плану реагування на інциденти IT-безпеки. Якщо компанія зазнає витоку даних в умовах відсутності надійної стратегії реагування, наслідки можуть бути катастрофічними.

Більшість МСП після витоку даних опиняються на межі банкрутства

Внаслідок витоків даних особливо сильно страждають малі й середні підприємства. Близько 60% таких компаній припиняють свою діяльність протягом шести місяців після кібератаки. Більша частина цієї шкоди пов'язана з фінансовими втратами. Але слід також враховувати вплив на репутацію. Після того, як стає відомо про порушення безпеки, надзвичайно важко відновити довіру клієнтів та інших зацікавлених сторін. Судові позови та штрафи також можуть ускладнити виживання МСП.

Більшість компаній занадто довго виявляють витоки інформації

Ситуації, коли організації занадто довго не можуть виявити атаку, можуть спричинити значні негативні наслідки для їх функціонування. Сьогодні більшості компаній потрібно більше шести місяців, щоб зрозуміти, що їх атакували. За цей час зловмисники можуть завдати великої шкоди, викравши конфіденційну інформацію або пошкодивши мережу. У таких випадках дуже важливими є системи аудиту та моніторингу. Якщо виникає вразливість або атака, компанії можуть дізнатися про це якомога швидше і вжити необхідних заходів, щоб мінімізувати збитки і захистити свій бізнес [10].

1.3 Види й механізми реалізації загроз інформаційній безпеці

Сучасні технології та постійне підключення до Інтернету відкривають більше можливостей, ніж будь-коли, водночас призводять до виникнення нових способів проникнення навіть у найбільш захищені мережі світу.

Загрози кібербезпеці відображають ризик кібератаки. Кібератака - це навмисні та зловмисні зусилля однієї організації або особи, спрямовані на порушення роботи систем іншої організації або особи. Цілі зловмисників включають крадіжку інформації, отримання фінансової вигоди, шпигунство та саботаж [8].

Розглянемо основні види загроз інформаційній та кібербезпеці (Рис. 1.6).

Рис. 1.6. Загрози інформаційній та кібербезпеці

1. Атаки шкідливого програмного забезпечення

Атаки використовують багато методів для потрапляння шкідливого програмного забезпечення на пристрій користувача, найчастіше - соціальну інженерію. Користувачів можуть попросити виконати певну дію, наприклад, перейти за посиланням або відкрити вкладення. В інших випадках шкідливе програмне забезпечення використовує вразливості в браузерах або операційних системах, щоб завантажитися самостійно без відома або згоди користувача.

Після встановлення шкідливе ПЗ може відстежувати дії користувача, надсилати зловмиснику конфіденційні дані, допомагати йому проникнути до інших цілей у мережі і навіть змусити пристрій користувача брати участь у бот-мережі, яка використовується зловмисником для організації інших атак.

Для кібератак використовують такі види шкідливого ПЗ:

- Троянський вірус - обманює користувача, змушуючи його думати, що це нешкідливий файл. Троянський вірус може запустити атаку на систему і встановити чорний хід, яким можуть скористатися зловмисники.
- Програми-вимагачі - перешкоджають доступу до даних жертви, погрожуючи видалити або опублікувати їх, якщо не буде сплачено викуп.

- Шкідливе програмне забезпечення-шифрувальник - має на меті знищити дані або системи, перезаписуючи цільові файли або знищуючи всю файлову систему. Зазвичай вони призначені для надсилання політичних повідомлень або приховування хакерських дій після викрадення даних.

- Хробаки - це шкідливе програмне забезпечення, призначене для використання бекдорів і вразливостей для отримання несанкціонованого доступу до операційних систем. Після інсталяції хробак може виконувати різні атаки, зокрема атаку з метою розподіленої відмови в обслуговуванні (DDoS).

- Шпигунські програми - це шкідливе ПЗ дозволяє зловмисникам отримати несанкціонований доступ до даних, включаючи конфіденційну інформацію, таку як платіжні реквізити й облікові дані. Шпигунські програми можуть вражати мобільні телефони, десктопні програми та десктопні браузери.

- Безфайлове шкідливе програмне забезпечення - цей тип шкідливого ПЗ не вимагає встановлення програмного коду в операційній системі. Він робить власні файли, такі як PowerShell і WMI, редагованими, щоб увімкнути шкідливі функції, що робить їх легітимними і складними для виявлення.

- Маніпуляції з додатками або веб-сайтами - OWASP окреслює 10 основних ризиків для безпеки додатків, починаючи від порушеного контролю доступу та неправильної конфігурації безпеки, закінчуючи ін'єкційними атаками та криптографічними збоями. Як тільки вектор встановлюється через набуття облікового запису сервісу, запускається більше шкідливого програмного забезпечення, атак на облікові дані або APT-атак [8].

2. Атаки соціальної інженерії

Соціоінженерні атаки працюють шляхом маніпулювання психікою користувачів, змушуючи їх виконувати бажані для зловмисника дії або розголошувати конфіденційну інформацію.

Атаки соціальної інженерії охоплюють:

- Фішинг - зловмисники надсилають шахрайську кореспонденцію, яка нібито надходить з легітимних джерел, зазвичай електронною поштою. Електронний лист може спонукати користувача виконати важливу дію або

перейти за посиланням на шкідливий веб-сайт, що призведе до передачі конфіденційної інформації зловмиснику або до завантаження шкідливого ПЗ. Фішингові електронні листи можуть містити вкладення, заражені шкідливим кодом.

- Цільовий фішинг - варіант фішингу, в якому зловмисники цілеспрямовано атакують осіб, які мають привілеї або вплив у сфері безпеки, наприклад, системних адміністраторів або керівників вищої ланки.
- Китобійний промисел - ця фішингова атака націлена на високопоставлених керівників («китів»), таких як головний виконавчий директор (CEO) або фінансовий директор (CFO). Зловмисник намагається обманом змусити жертву розкрити конфіденційну інформацію.
- Шкідлива реклама - контрольована хакерами реклама в Інтернеті, яка містить шкідливий код, що заражає комп'ютер користувача, коли він натискає на неї або навіть просто переглядає оголошення. Слід зазначити, що зловмисна реклама була виявлена на багатьох провідних Інтернет-виданнях.
- Drive-by завантаження - зловмисники можуть зламувати веб-сайти і вставляти шкідливі скрипти в PHP або HTTP-код сторінки. Коли користувачі відвідують сторінку, шкідливе ПЗ безпосередньо встановлюється на їхній комп'ютер; або ж скрипт зловмисника перенаправляє користувачів на шкідливий сайт, який виконує завантаження. Drive-by завантаження використовують вразливості браузерів або операційних систем.
- Залякувальне програмне забезпечення - вдає, що сканує комп'ютер на наявність шкідливого коду, а потім регулярно показує користувачеві фальшиві попередження та виявлення. Зловмисники можуть попросити користувача заплатити, щоб видалити фальшиві загрози з комп'ютера або зареєструвати ПЗ. Користувачі, які погоджуються, передають зловмиснику свої фінансові дані.
- Приманка – атака відбувається, коли суб'єкт нападу обманом змушує жертву використовувати шкідливий пристрій, розміщуючи заражений шкідливим програмним забезпеченням фізичний пристрій, наприклад, USB, там,

де жертва може його знайти. Коли жертва вставляє пристрій у свій комп'ютер, вона ненавмисно інсталює шкідливе програмне забезпечення.

- Вішинг - голосові фішингові атаки використовують методи соціальної інженерії, щоб змусити жертву розкрити фінансову або особисту інформацію по телефону.
- Вигадка – атака відбувається, коли суб'єкт загрози обманює жертву, щоб отримати доступ до привілейованих даних. Шахрайство під хибним приводом може полягати в тому, що зловмисник вдає, що підтверджує особу жертви, запитуючи фінансові або персональні дані.
- Залякування - зловмисник змушує жертву думати, що вона ненавмисно завантажила незаконний контент або що її комп'ютер заражений шкідливим програмним забезпеченням. Потім зловмисник пропонує жертві рішення для усунення хибної проблеми, змушуючи жертву завантажити і встановити шкідливе програмне забезпечення.
- Крадіжка з відволікаючим маневром - зловмисники використовують соціальних інженерів, щоб обдурити кур'єра або компанію доставки, змусивши його поїхати в неправильне місце доставки або забрати товар, перехопивши транзакцію.
- Медова пастка (Honey trap) - соціальний інженер видає себе за привабливу особу, щоб взаємодіяти з жертвою в Інтернеті. Соціальний інженер фальсифікує онлайн-відносини і збирає конфіденційну інформацію через ці відносини.
- «За хвостом» (Tailgating або piggybacking) - відбувається, коли суб'єкт загрози проникає в будівлю, що охороняється, йдучи слідом за уповноваженим персоналом. Зазвичай працівники, які мають законний доступ, припускають, що людині, яка стоїть позаду, дозволено увійти, і притримують для неї двері.
- Фармінг - схема онлайн-шахрайства, під час якої кіберзлочинець встановлює шкідливий код на сервер або комп'ютер. Код автоматично

перенаправляє користувачів на фальшивий веб-сайт, де їх обманом змушують надати персональні дані [11].

3. Атаки на ланцюжок постачання програмного забезпечення

Атака на ланцюжок постачання програмного забезпечення - це кібератака на організацію, спрямована на слабкі ланки в ланцюжку оновлення та постачання ПЗ, якому вона довіряє. Ланцюг постачання - це мережа всіх осіб, організацій, ресурсів, видів діяльності й технологій, що беруть участь у створенні та продажу продукту. Атака на ланцюжок постачання ПЗ використовує довіру, яку компанії мають до своїх постачальників, особливо щодо оновлень і виправлень.

Часто це стосується інструментів мережевого моніторингу, промислових систем управління, «розумних» машин та інших мережевих систем зі службовими обліковими записами. Атака може бути здійснена в багатьох місцях проти життєвого циклу програмного забезпечення безперервної інтеграції та безперервної доставки (CI/CD) постачальника або навіть проти сторонніх бібліотек і компонентів, як це видно на прикладі Apache і Spring [12].

Типи атак на ланцюжок постачання програмного забезпечення:

- Компрометація інструментів створення програмного забезпечення або інфраструктури розробників/тестувальників.
- Компрометація пристроїв або облікових записів, що належать привілейованим стороннім постачальникам.
- Шкідливі програми, підписані викраденими сертифікатами підпису коду або ідентифікаторами розробника.
- Розгортання шкідливого коду на апаратному чи програмному забезпеченні.
- Шкідливе програмне забезпечення, попередньо встановлене на таких пристроях, як камери, USB-накопичувачі та мобільні телефони [8].

4. Сучасні постійні загрози (APT)

Коли особа або група осіб отримує несанкціонований доступ до мережі і залишається невиявленою протягом тривалого періоду часу, зловмисники можуть викрасти конфіденційні дані, навмисно уникаючи виявлення службою

безпеки організації. APT вимагають витончених умінь та засобів, а також значних зусиль, тому вони, як правило, спрямовані проти національних держав, великих корпорацій або інших особливо цінних об’єктів.

До загальних індикаторів реалізації APT відносять:

- Створення нового облікового запису – «P» у слові «постійний» означає, що зловмисник створив ідентифікатор або обліковий запис у мережі з підвищеними привілеями.
- Аномальна активність - легітимні облікові записи користувачів зазвичай діють за шаблонами. Аномальна активність цих облікових записів може свідчити про наявність APT, зокрема, неактивний обліковий запис, який був створений, а потім деякий час не використовувався, і раптом став активним.
- Використання бекдорів/троянських коней - широке використання цього методу дозволяє зберігати довготривалий доступ до облікового запису.
- Нетипова активність бази даних - наприклад, раптове збільшення кількості операцій з базою даних з великими обсягами даних.
- Незвичайні файли даних - наявність таких файлів може вказувати на те, що дані були об'єднані у файли для полегшення процесу викрадення [8].

5. Розподілена відмова в обслуговуванні (DDoS)

Мета атаки типу «відмова в обслуговуванні» (DoS) - перевантажити ресурси цільової системи і змусити її припинити роботу, позбавивши доступу до неї користувачів. Розподілена відмова в обслуговуванні (DDoS) - це варіант DoS-атаки, в якому порушники компрометують велике число комп'ютерів або інших пристроїв і використовують їх у скоординованій атаці проти цільової системи.

DDoS-атаки часто використовуються в поєднанні з іншими кіберзагрозами. Ці атаки можуть запускати відмову в обслуговуванні, щоб привернути увагу співробітників служби безпеки і створити плутанину, в той час як вони здійснюють більш витончені атаки, спрямовані на крадіжку даних або заподіяння іншої шкоди.

До методів DDoS-атак відносять:

- Ботнети - системи під контролем хакерів, які були заражені шкідливим ПЗ. Зловмисники використовують цих ботів для здійснення DDoS-атак. Великі ботнети можуть включати мільйони пристроїв і здійснювати руйнівні атаки.

- Smurf-атака - надсилає на IP-адресу жертви ехо-запити за протоколом ICMP (Internet Control Message Protocol - протокол керуючих інтернет-повідомлень). ICMP-запити генеруються з «підроблених» IP-адрес. Зловмисники автоматизують цей процес і виконують його в масштабі, щоб перевантажити цільову систему.

- TCP SYN flood атака - атаки засипають цільову систему запитами на з'єднання. Коли цільова система намагається завершити з'єднання, пристрій зловмисника не відповідає, змушуючи цільову систему очікувати. Це швидко заповнює чергу на з'єднання, не даючи змоги підключитися авторизованим користувачам.

6. Атака «людина посередині» (Man-in-the-middle, MitM)

Коли користувачі або пристрої отримують доступ до віддаленої системи через Інтернет, вони вважають, що спілкуються безпосередньо з сервером цільової системи. Під час MitM-атаки зловмисники порушують це припущення, розміщуючись між користувачем і цільовим сервером.

Після того, як зловмисник перехопив комунікацію, він може скомпрометувати облікові дані користувача, викрасти конфіденційні дані та повернути користувачеві різні відповіді.

До MitM-атак відносяться:

- Перехоплення сеансу - зловмисник перехоплює сеанс між мережевим сервером і клієнтом. Комп'ютер, що атакує, підміняє свою IP-адресу на IP-адресу клієнта. Сервер вважає, що він зв'язується з клієнтом, і продовжує сеанс.

- Повторна атака - кіберзлочинець підслуховує мережеве спілкування і відтворює повідомлення пізніше, видаючи себе за користувача. Повторні атаки були значною мірою пом'якшені додаванням міток часу до мережевих повідомлень.

- Підміна IP-адреси - зловмисник переконує систему, що вона листується з надійним, відомим суб'єктом. Таким чином, система надає зловмиснику доступ.

Зловмисник підробляє свій пакет з IP-адресою джерела довіреного хоста, а не власною IP-адресою.

- Атака на підслуховування - зловмисники використовують незахищений мережевий зв'язок для доступу до інформації, що передається між клієнтом і сервером. Ці атаки важко виявити, оскільки мережеві передачі виглядають типовими.

- Атаки через Bluetooth - оскільки Bluetooth часто відкритий у увімкненому режимі, існує багато атак, особливо на телефони, які скидають контактні картки та інше шкідливе програмне забезпечення через відкриті та приймаючі Bluetooth - з'єднання. Зазвичай така компрометація кінцевої точки є засобом для досягнення мети, від збору облікових даних до особистої інформації [13].

7. Атаки на паролі

Хакер може отримати доступ до інформації про пароль користувача, «винюхуючи» з'єднання з мережею, використовуючи соціальну інженерію, вгадуючи або отримуючи доступ до бази даних паролів. Зловмисник може «вгадати» пароль випадковим або систематичним чином.

До парольних атак відносяться:

- Підбір пароля методом грубої сили - зловмисник використовує програмне забезпечення, щоб спробувати багато різних паролів, сподіваючись вгадати правильний. Програмне забезпечення може використовувати певну логіку для підбору паролів, пов'язаних з іменем людини, її роботою, сім'єю тощо.

- Словникова атака - для отримання доступу до комп'ютера та мережі жертви використовується словник поширених паролів. Один із методів полягає в тому, щоб скопіювати зашифрований файл, який містить паролі, застосувати таке ж шифрування до словника паролів, які регулярно використовуються, і порівняти отримані результати.

- Атака на хеш - зловмисник використовує протокол автентифікації під час сеансу і перехоплює хеш пароля (на відміну від безпосередньо символів пароля), а потім передає його для автентифікації та латерального доступу до

інших мережевих систем. У цих типах атак зловмиснику не потрібно розшифровувати хеш, щоб отримати звичайний текстовий пароль.

- Атака «золотого квитка» - починається так само, як і атака передачі хешу, коли в системі Kerberos (Windows AD) зловмисник використовує викрадений хеш пароля для доступу до центру розподілу ключів, щоб підробити хеш TGT-квитка, що видає квиток . Цей вектор атаки часто використовується в мімікрованих атаках [14].

Висновки до розділу 1

Під інформаційною безпекою будемо розуміти захищеність інформації й інфраструктури, яка її підтримує від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати неприйнятної шкоди суб'єктам інформаційних відносин. Інформаційна безпека має чотири основні принципи: конфіденційність, цілісність, доступність і неспростовність.

Дослідження показало, що управління інформаційною безпекою передбачає розроблення, впровадження, функціонування, моніторинг, перегляд, підтримку і вдосконалення інформаційної безпеки організації і реалізується шляхом впровадження комплекс адміністративних, фізичних і технічних заходів.

З’ясовано, що загрози інформаційній безпеці - це дії або події, які потенційно можуть порушити конфіденційність, цілісність або доступність даних чи систем і походити з різних джерел, зокрема від окремих осіб, груп, технічних пристроїв, програм або природних явищ

Встановлено, що основними джерелами загроз інформаційній безпеці антропогенного характеру є держави; терористичні організації; промислові шпигуни; організовані злочинні угруповання; хакери; хактивісти; зловмисні інсайдери. Загрози інформаційній та кібербезпеці включають такі види: шкідливе ПЗ; соціальна інженерія; загрози ланцюжку постачання ПЗ; сучасні постійні загрози (APT); DDoS-атаки; атаки MitM, злам паролів.

Розділ 2 ОСНОВНІ ЗАСАДИ РОЗВІДКИ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА

Розвідка загроз є важливим елементом не тільки менеджменту інформаційної безпеки, але й невід'ємною частиною стратегічного управління сучасною компанією, що дозволяє їй забезпечити безпеку своїх активів і зберегти конкурентну перевагу в умовах зростання інформаційних загроз.

2.1 Сутність і основні принципи розвідки загроз

Виявлення загроз в управлінні корпоративною інформацією є критично важливим з двох основних причин: забезпечення безпеки та збереження конкурентних переваг.

Інформація є одним з найцінніших активів компанії. Розвідка загроз може допомогти запобігти та виявити потенційні атаки, такі як кіберзлочини, шпигунство та витік даних. Завдяки всебічному аналізу та розумінню потенційних загроз можна розробити і впровадити ефективні заходи захисту, знизивши таким чином ризик втрати конфіденційної інформації та шкоди діловій репутації.

У сучасному бізнес-середовищі, де посилюється конкуренція, особливо в цифровому просторі, розвідка загроз може допомогти компаніям виявити потенційні ризики, використати конкурентну розвідку для формування стратегій розвитку та запобігти можливим негативним наслідкам дій конкурентів. Тобто розвідка загроз є потенційним інструментом збереження конкурентних переваг бізнесу й утримання вигідної позиції на ринку.

Що ж таке розвідка загроз (кіберзагроз)? Розвідка загроз (аналіз загроз) є важливим елементом інформаційної безпеки, який допомагає заздалегідь визначити, які загрози є найбільш небезпечними для конкретного бізнесу. Таким чином можна виявити загрози, які сплановані або вже націлені на організацію, її співробітників, клієнтів і партнерів. Ці загрози можуть призвести до втрати

доходів, шкоди репутації, перебоїв у наданні послуг та інших негативних наслідків.

Розвідка загроз дозволяє організаціям визначати пріоритети найбільш імовірних причин проблем і спрямовувати наявні ресурси туди, де вони можуть бути найбільш ефективними.

Розвідка кіберзагроз (Cyber Threat Intelligence, CTI) - це процес збору, обробки та аналізу інформації про існуючі та нові загрози, які можуть бути спрямовані на організацію.

За визначенням Gartner, розвідка загроз - це засновані на фактах знання про існуючу або загрозу, що виникає, або небезпеку для ресурсів, якими можна керуватися як при розробці політики безпеки, так і при проектуванні мереж.

Розвідка загроз діє як проактивний захід безпеки, запобігає витоку даних і зменшує фінансові витрати на відновлення після інцидентів. CTI збирає інформацію про кіберзагрози та суб'єктів загроз і використовує різні джерела для їх ідентифікації. Процес розвідки загроз охоплює дослідження, аналіз і моделювання для запобігання та виявлення атак.

Розвідка загроз (кіберзагроз) - це дисципліна, яка розвивається й надає організаціям науково обґрунтовану інформацію про потенційні загрози інформаційним активам та інфраструктурі, включаючи нові кіберзагрози, а також забезпечує компанію інформацією, необхідною для проактивного зміцнення її захисту та прийняття обґрунтованих рішень з питань безпеки.

Розвідка загроз як ефективний інструмент забезпечення кібербезпеки організації, підприємства чи установи забезпечує:

1. Виявлення й аналіз кіберзагроз і забезпечення проактивного та обґрунтованого захисту.

2. Вихід за рамки простого збору даних про загрози.

3. Надання комплексного бачення, яке поєднує докази і контекст.

4. Управління стратегією кібербезпеки організації [15].

Інтерпретація розвідданих про загрози дозволяє організаціям зрозуміти ризики, з якими вони стикаються, і вжити запобіжних заходів для зменшення потенційної шкоди.

Ефективна розвідка загроз ґрунтується на всебічній інформації і потребує поєднання та контекстуалізації різних типів даних, зібраних з багатьох різноманітних джерел, для отримання дієвих висновків. Зокрема, розвідка загроз використовує дані з внутрішніх систем, засобів контролю безпеки та хмарних сервісів, які складають основу надійної програми розвідки загроз.

Мета полягає в тому, щоб надати як докази того, що загрози є реальними, так і практичні висновки, які забезпечать ефективні способи боротьби з ними.

Основними причинами важливості розвідки загроз безпеці визначають такі (Рис. 2.1.):

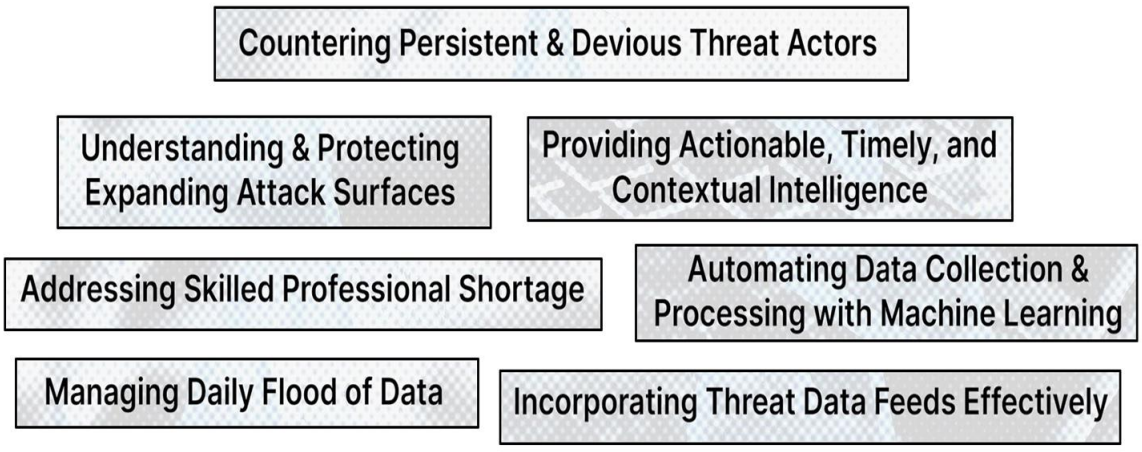

Рис. 2.1. Основні причини важливості розвідки загроз

1. Протидія постійним та підступним суб'єктам загроз.

2. Управління щоденним потоком даних.

3. Вирішення проблеми нестачі кваліфікованих фахівців.

4. Розуміння та захист зростаючих поверхонь атак.

5. Ефективне поєднання потоків даних про загрози.

6. Автоматизація процесів збору й обробки даних за допомогою машинного навчання.

7. Забезпечення дієвої, своєчасної та пов’язаної з контекстом розвідки.

Розглянемо основні завдання розвідки загроз на прикладі її успішного

застосування в компаній. Отже, в центрі уваги велика міжнародна фінансова організація із мільярдними активами, в якій відбувається ретельно сплановане порушення кібербезпеки. Групі висококваліфікованих хакерів вдалося практично не залишили слідів свого вторгнення в корпоративну мережу й уникнути виявлення. Відповідно, в компанії не мають найменшого уявлення про цю критично важливу подію.

Саме в такій і подібних ситуаціях розвідка загроз є незамінною, забезпечуючи виконання таких завдань (Рис. 2.2):

Рис. 2.2. Завдання розвідки загроз

1. *Раннє виявлення* в результаті безперервного моніторингу мережі компанії, у процесі якого відбувається збір даних із різних джерел, включаючи відкриті джерела, внутрішні журнали й індикатори загроз. Виявлення непритаманних мережевому трафіку закономірностей, підозрілих дій і неочікуваного збільшення обсягу доступу до даних викликають сигнали тривоги. В іншому випадку ці малопомітні відхилення можуть залишитися непоміченими.

2. *Атрибуція та контекст*: розвідка загроз визначає походження атаки і приписує її відомому кіберзлочинному угрупованню з історією фінансових махінацій. Контекстні відомості, зокрема про тактику, методи та процедури (TTPs) зловмисного суб’єкта чи групи суб’єктів, має вирішальне значення для розуміння характеру загрози.

3. *Усунення наслідків і реагування*: Отримавши актуальну інформацію, аналітики загроз кібербезпеки організації оперативно реагують на загрозу,

впроваджуючи заходи протидії з урахуванням конкретної тактики зловмисників. Крім того, розвідка загроз надає рекомендації щодо запобігання потенційних загрозам, завдяки чому організація може усунути вразливості та зміцнити захист.

4. *Обмін інформацією*: завдяки розвідці загроз компанія має можливість поділитися отриманими даними про загрози й порушників безпеки з іншими організаціями та службами кібербезпеки, створюючи умови для спільної боротьби з кіберзлочинністю, запобігання й ефективного реагування на кіберзагрози. Такий обмін даними про загрози необхідний для створення колективного захисту від загроз, які постійно ускладнюються і розвиваються.

5. *Безперервний моніторинг*: Навіть після того, як початковий інцидент локалізований, розвідка загроз продовжує вести моніторинг 24\7 [16].

2.2 Етапи і джерела інформації розвідки загроз

Аналіз розвідувальних даних про кіберзагрози може бути непростим завданням. Часто будучи перевантаженими даними, потопаючи в перехресних посиланнях, фахівцям важко зрозуміти, з чого почати і коли закінчити аналіз. Щоб допомогти аналітикам орієнтуватися в цьому лабіринті, спецслужби по всьому світу використовують життєвий цикл розвідки загроз.

Життєвий цикл розвідки - це структурований підхід до збору, аналізу та поширення розвідувальної інформації. Він слугує шаблоном для аналітиків, якого вони дотримуються під час збору та використання розвідувальних даних. Індустрія кібербезпеки адаптувала цей життєвий цикл до власних потреб і створила життєвий цикл розвідки кіберзагроз (CTI).

Життєвий цикл розвідданих про кіберзагрози - це модель, яку можна використовувати для структурування аналізу розвідданих від початку до кінця. Використовуючи цю модель, можна структурувати процес збору, аналізу та розповсюдження розвідданих про загрози серед ключових зацікавлених сторін в організації [17].

Цей життєвий цикл відповідає ідеалізованій моделі того, як західні розвідувальні організації структурують свої розвідувальні операції від збору до розповсюдження. Цей життєвий цикл може бути використаний як керівництво для аналітиків CTI в їхній роботі або як шаблон для менеджерів CTI при формулюванні процесів для своїх команд.

Життєвий цикл розвідки загроз складається з шести етапів (Рис. 2.3): планування, збір, обробка, аналіз, поширення та зворотній зв'язок [18].

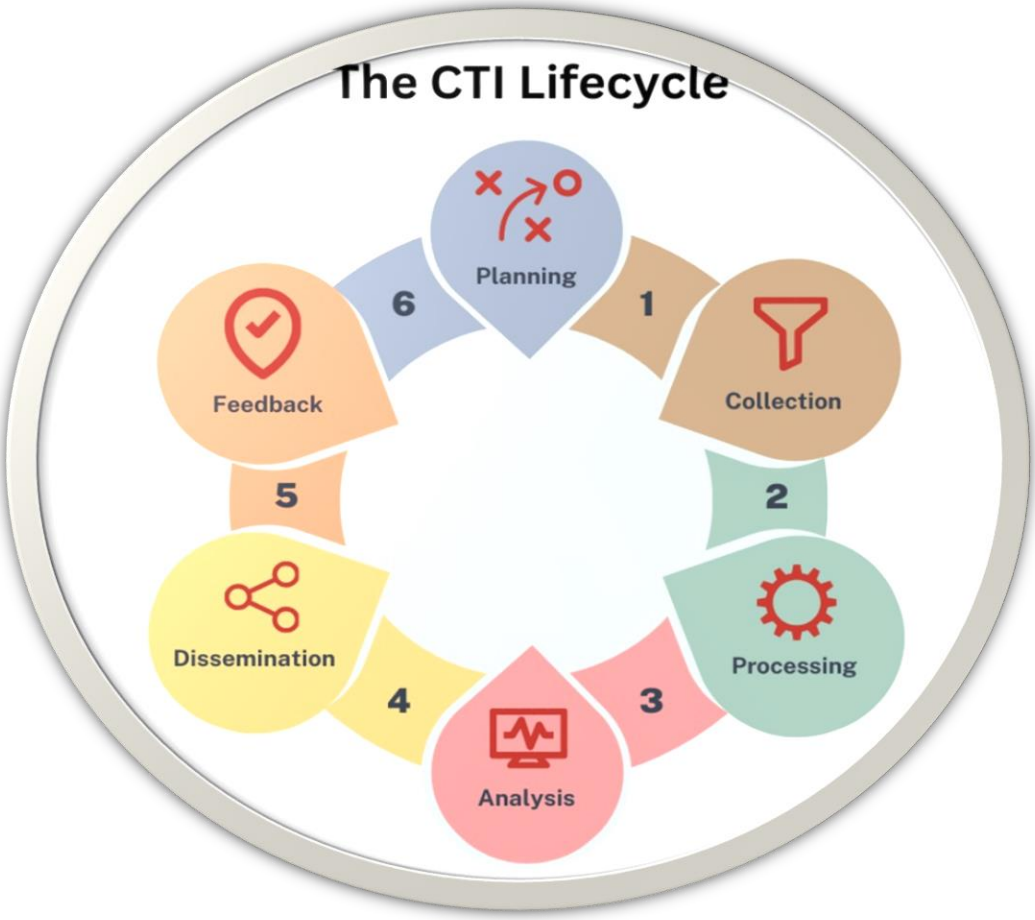

Рис. 2.3. Життєвий цикл розвідки загроз.

Етап 1: Планування.

Першим етапом життєвого циклу розвідки загроз є планування. На цьому етапі організація визначає цілі й завдання діяльності з розвідки загроз або планує загальні цілі програми.

На цьому етапі необхідно здійснити таке:

1. Визначити ключові зацікавлені сторони, з якими буде здійснюватися обмін розвідувальними даними, і як це буде досягнуто.

2. Визначити потреби організації в розвідувальних даних, зосередившись на поточних загрозах на оперативному рівні та оцінюючи майбутні загрози на стратегічному рівні.

3. Визначити сферу застосування та основні цілі програми CTI. Це може сильно відрізнятися від організації до організації. Наприклад, одна організація може прагнути захистити репутацію свого бренду, інша – захистися від програм-вимагачів, а оборонний підрядник - відстежувати сучасні постійні загрози (APT).

4. Визначити пріоритетні об’єкти, які підлягають захисту, насамперед конфіденційна інформація, критичні операції та активи.

5. Виявити існуючі прогалини в розвідці. Якщо стратегічні цілі змінилися або були виявлені прогалини в минулій розвідувальній діяльності, усунення цих прогалин має стати пріоритетом. Це може передбачати збір більшої кількості або інших даних, зміну методів обробки і аналізу або коригування методів поширення інформації.

Наприкінці цього етапу слід розробити план, який детально описує, як аналітики збиратимуть, аналізуватимуть і поширюватимуть інформацію для задоволення потреб організації в розвідданих.

Етап 2: Збір даних.

Після того, як план підготовлено, можна приступати до етапу збору інформації. Цей етап передбачає збір інформації, яка відповідає попередньо визначеним інформаційним потребам організації. Сюди входить визначення відповідних джерел даних для збору та зберігання інформації.

Існує багато способів збору розвідданих про кіберзагрози. Залежно від джерел даних, доступних для організації, вони можуть включати такі:

– Отримання метаданих і журналів з інструментів безпеки та мереж організації.

– Збір розвідданих про загрози з комерційних або відкритих каналів розвідки загроз, на які підписана організація.

– Безпосередня взаємодія з обізнаними джерелами, такими як журналісти, інсайдери та колеги.

– Аналіз новин, блогів та інших відкритих джерел OSINT.

– Вилучення даних із соціальних мереж, веб-сайтів і форумів.

Етап 3: Обробка даних.

Зібравши необроблені дані, організація має належним чином обробити їх, щоб перетворити на інформацію для аналізу. На етапі обробки аналітики організують і структурують зібрані дані, щоб підготувати їх до аналізу. Цей етап передбачає:

– Очищення даних, щоб видалити будь-яке сміття.

– Нормалізацію даних, щоб їх можна було завантажити до корпоративного рішення для зберігання даних.

– Перевірка законності та достовірності даних на основі джерела, з якого їх зібрано, і того, що про них говорять інші. Наприклад, чи визнають IP-адресу зловмисною кілька постачальників розвідувальних даних або ніхто, окрім автора публікації в блозі, де інформація була знайдена.

– Обробка зібраних даних є життєво важливою для забезпечення ефективного аналізу. Якщо аналізу підлягають недостовірні й неактуальні або взагалі фейкові дані, висновки будуть хибними й невартими довіри.

– Використання для збору розвідданих даркнету, наприклад, інформації, які циркулює на форумах темної мережі та інших каналів, якими послуговуються кіберзлочинці для отримання даних.

Водночас, слід пам’ятати, що не всі дані можна зібрати. Місце функціонування організації визначає її операційне середовище, яке базується на культурних, технологічних та геополітичних факторах. Операційне середовище визначає, до яких джерел даних можна отримати доступ і які загрози можна побачити. Наприклад, охоронна компанія, яка збирає інформацію від клієнтів у США, бачитиме зовсім інші дані й загрози, ніж охоронна компанія в Ірані.

Компанія може зібрати підмножину даних, доступних у її робочому середовищі, використати підмножину цих даних для отримання розвідданих (на етапі обробки) і використати їх для отримання розвідданих (на етапі аналізу). У

міру того, як організація рухається життєвим циклом, обсяг даних, інформації та аналітики стає все меншим і меншим.

Етап 4: Аналіз інформації.

На етапі аналізу зібрана інформація перетворюється на дієві розвідувальні дані, які можуть бути використані для захисту організації та прийняття стратегічних рішень. На цьому етапі спеціалісти-аналітики використовують свої знання і досвід для виявлення закономірностей і тенденцій у зібраній інформації. Виявлені закономірності інтерпретуються і надають інформацію, яку організація може використати в процесі прийняття рішень.

Розуміння характеру, масштабу та наслідків загроз, що містяться в зібраних даних, є кінцевою метою цього етапу. Аналітик CTI є ключовим інтерпретатором у формулюванні дієвих розвідувальних даних.

На цьому етапі організація може використовувати різноманітні методи й інструменти структурованого аналізу (наприклад, діамантову модель [19], кіберланцюг вбивств [20] тощо).

Етап 5: Поширення інформації.

Після того, як фахівці з аналізу перетворили зібрані дані на дієву інформацію, організація має поділитися нею з відповідними зацікавленими сторонами.

Це один з ключових етапів життєвого циклу розвідки загроз, який потрібно пройти правильно. Компанія може володіти найкращими розвідданими у світі, які можуть врятувати її від неминучої атаки або повернути програму кібербезпеки на правильний шлях. Однак така інформація буде марною, якщо не буде вчасно передана всім зацікавленим сторонам. Стейкхолдери – це фізичні та юридичні особи, які мають законний інтерес у діяльності організації і, відповідно, певною мірою залежать від неї або можуть впливати на її діяльність.

Доцільно зробити етап поширення розвідданих максимально автоматизованим через автоматичне завантаження ІОД для виявлення на платформу SIEM або EDR, використання заздалегідь визначених шаблонів при написанні електронних листів, звітів або презентацій, а також створення групи

для обміну інформацією, щоб не потрібно було контактувати з кожною зацікавленою стороною індивідуально.

Етап 6: Зворотний зв'язок

Етап, яким часто нехтують у життєвому циклі розвідки загроз, - це етап зворотного зв'язку. Кожен аналітик CTI прагне збирати, аналізувати й ділитися розвідданими. Однак, вони менш зацікавлені в отриманні зворотного зв'язку про ефективність своїх зусиль або про те, чи є розвіддані, які вони використовують або виробляють, корисними.

Етап зворотного зв'язку має вирішальне значення, якщо компанія прагне, щоб корпоративна діяльність в галузі автоматизованих інформаційних систем (AIC). AIC - це комплексні системи, які автоматизують обробку, зберігання та передачу інформації. Вони можуть включати в себе різні компоненти, такі як сервери, бази даних, мережеві пристрої, програмне забезпечення та інші елементи) постійно вдосконалювалася і приносила користь. Організація має знати, чи впливають її зусилля в галузі AIT на діяльність операційного чи стратегічного рівня, і якщо ні, то як скоригувати ситуацію, щоб вони впливали.

Занадто часто команди CTI сліпо діляться розвідданими з людьми у своїй організації і ніколи не замислюються над тим, чи додає цінності те, чим вони діляться. Компанії потрібен двосторонній канал зв'язку між командою CTI та ключовими зацікавленими сторонами. Зацікавлені сторони мають надавати зворотній зв'язок щодо ефективності розвідувальних даних, якими вони діляться, як вони їх використовують, і чи можна зробити якісь покращення, щоб допомогти у прийнятті обґрунтованих рішень.

Розвідка загроз збирає дані з багатьох джерел, які, зазвичай, поділяють на зовнішні і внутрішні. Внутрішня розвідка загроз передбачає, що організації отримують і аналізують дані зі своїх мереж, включаючи журнали подій і програм, журнали брандмауера, журнали DNS та інші джерела. Компанії також можуть зберігати інформацію про минулі події безпеки, щоб допомогти отримувати додаткові дані про загрози. Це може включати дані про системи, які постраждали в результаті інциденту, конкретні вразливості, які використав

зловмисник, і показники компрометації (IoC), що були виявлені, а також дані пакетів та інші необроблені допоміжні дані.

Зовнішня розвідка загроз передбачає отримання інформації про загрози з різних джерел за межами організації. Це може включати загальнодоступну інформацію з відкритим кодом, як-от блоги, новини, загальнодоступні списки блокувань, приватні чи комерційні джерела, такі як постачальники програмного забезпечення для аналізу загроз, і навіть корпоративні групи обміну, які погодилися об’єднати інформацію про потенційні загрози кібербезпеці [21].

Відповідно до [22] розвіддані, отримані з внутрішніх джерел, охоплюють події, які відбулися у внутрішній мережі організації та на хостах. Останні можуть надавати індикатори про те, що загрози перетнули периметр безпеки, порушили внутрішні правила контролю доступу, заразили систему або спробували отримати доступ до обмеженої системи.

Статистичні дані забезпечують базову лінію нормальної поведінки, щоб будь-яку аномалію можна було висвітлити та дослідити.

До *внутрішніх джерел CTI* відносять такі (Рис. 2.4):

Системні журнали та події. Така інформація широко доступна на пристроях і в програмах; її можна легко переслати до центрального об’єкта за допомогою таких інструментів, як Syslog або Windows event forwarding (WEF). Оскільки до CTI застосовуються лише певні повідомлення журналу та події, будь-яка централізована система журналювання, наприклад, система управління інцидентами та подіями безпеки (SIEM), повинна застосовувати фільтри та набори правил для отримання CTI.

CTI	Systems	Description
System logs and events	All systems	System activity, principally errors and security events
Network events	Network equipment, (switches, routers, firewalls)	devices connecting/disconnecting, ACL alert, login/failed login, etc.
Network utilisation and traffic profiles	Network equipment, (switches, routers, probes)	SNMP, NetFlow, RMON, etc. to Network management platform
Alerts from boundary devices	IDS/IPS, Firewall, WAF	Alerts/events collected and analysed by SIEM or vendor-specific management portal
AV, system alerts	Corporate AV software installed on host systems, (client and Server)	Corporate AV system alerts from host AV software
Human	All systems	Observed anomalies or events
Forensic	All systems	Artefacts and intelligence gathered after an event

Рис. 2.4. Внутрішні джерела даних для розвідки загроз

Мережеві події. Мережеві пристрої, такі як маршрутизатори, комутатори та брандмауери, підтримують простий протокол керування мережею (SNMP), який можна використовувати для надсилання (майже в реальному часі) повідомлень про події, відомих як пастки SNMP, на центральний сервер для обробки. Перехоплення SNMP можна налаштувати для різноманітних подій CTI у внутрішній мережі (наприклад, запит на підключення, подія входу тощо).

Профілі використання мережі та трафіку. Це може свідчити про ненормальну поведінку, як-от ненадійний або надмірний трафік від клієнта або між клієнтами. Статистика доступна в багатьох формах, від простих лічильників у SNMP і Remote MONitoring (RMON) до детальних даних IP і протоколу з NetFlow і аналогічних комутаторів і зондів.

Граничні пристрої безпеки. На додаток до вищевказаних подій, пропрієтарні граничні пристрої безпеки, такі як системи запобігання вторгненню в мережу (NIDS) і брандмауери веб-додатків (WAF), можуть мати власну консоль керування для конкретної програми, яка також передає події безпеки в SIEM.

Антивірусні системи. Корпоративні антивірусні системи повідомляють про випадки зловмисного програмного забезпечення на центральну консоль, що забезпечує повне охоплення хостів в організації; як і з обмежувальними пристроями, це також може передавати події безпеки в SIEM.

Люди. Персонал організації часто найшвидше розпізнає, що щось не так; здатність швидко виявляти події та повідомляти про них - це те, чого можна досягти завдяки обізнаності користувачів і безперервному професійному навчанню безпеки.

Дані криміналістики. Містять артефакти, зібрані під час розслідування після інциденту безпеки, і можуть бути використані для посилення захисту безпеки. Аналіз заражених систем і файлів журналів може надати детальні відомості про тактику, прийоми та процедури (TTP), використані під час атаки.

Розвіддані з загальнодоступних зовнішніх джерел з відкритим кодом (OSINT) охоплюють: повідомлення про великий витік даних користувача, які можуть бути використані для доступу до інших систем, у фішингових атаках або геополітичній напруженості, що може збільшити ризик кібератаки. На рис. 2.5 показано основні зовнішні відкриті джерела CTI.

Source	Description
News feeds	News articles covering ongoing threats
Vulnerability	Alerts and advisories
Search automation	Using search technologies to find vulnerable systems: Google dorks, Shodan, etc.
Anti-virus vendors	Information, alerts, news feeds on malware activity and threats
Communications	Monitoring communication channels for intelligence: Slack, IRC, Twitter, etc.
Dark web	Intelligence available directly from the criminal underworld

Рис. 2.5. Зовнішні відкриті джерела CTI.

Велика кількість даних для розвідки загроз була доступна з каналів новин, сповіщень, постачальників антивірусів (AV) тощо. У більшості випадків вона також була доступна у форматі RSS, який є машиночитаним; однак вміст новин або сповіщень зазвичай містить посилання, що перенаправляє на веб-сторінку вільного формату, яку нелегко піддавати автоматизованому використанню та розумінню, незважаючи на значні досягнення в області обробки природної мови (NLP) і штучного інтелекту (AI). Типовими прикладами таких джерел серед інших є CERT-EU, Krebs on security, SANS інститут.

Повідомлення та сповіщення про вразливості є джерелами, що мають стандартизований формат CTI, у багатьох випадках із використанням загальних вразливостей і прогалин (CVE) і переліку загальних слабких місць (CWE), а

також загальної системи звітування про вразливості (CVRF). Типовими прикладами таких джерел є національна база даних уразливостей (NVD), поради щодо безпеки Cisco, портал безпеки Microsoft, поради щодо безпеки Oracle, поради щодо безпеки Red Hat, SecurityFocus тощо.

На відміну від попереднього типу зовнішніх джерел, останні містять (або можуть легко генерувати) активну інформацію про безпеку. Наприклад, канали даних NVD, окрім надання докладної інформації про передумови та вплив уразливості також містять мітки будь-яких зовнішніх посилань, таких як експлойт, виправлення, пом’якшення, технічний опис і продукт, які можуть керувати інструменти, що автоматизують вилучення корисної інформації.

Пошук у даркнеті зосереджується, зазвичай, на пошуку інтелектуальних даних, інструментів і послуг, недоступних у поверхневій мережі. Наприклад, можна здійснювати пошук за допомогою браузера TOR, який працює на одноразовій віртуальній машині, щоб забезпечити певну ізоляцію від шкідливого вмісту. Водночас, слід пам’ятати про проблеми швидкості й надійності підключень до сайтів [22].

2.3 Види розвідки загроз: стратегічна, оперативна, тактична

У широкому розумінні, потреби компанії в розвідданих будуть підпадати під один з трьох основних типів розвідки загроз: оперативну, тактичну або стратегічну (Рис. 2.6).

Оперативна розвідка загроз спрямована на неочікувані й існуючі ризики, зусилля щодо виявлення і реагування на які необхідно пріоритезувати. Отримані розвіддані охоплюють індикатори компрометації, сигнатури шкідливого ПЗ, зразки атак.

Тактична розвідка загроз пов'язана з технічними деталями конкретних загроз, таких як вразливості та експлойти. Тактична розвідка використовується для інженерії виявлення. Розвіддані охоплюють тактики, методи й процедури зловмисників (TTP), докази використання експлойтів.

Стратегічна розвідка загроз надає високорівневий огляд ландшафту загроз для формування ширших стратегій безпеки і пріоритетів у розподілі ресурсів. Розвіддані охоплюють знання про мотиви, можливості й тенденції розвитку загроз.

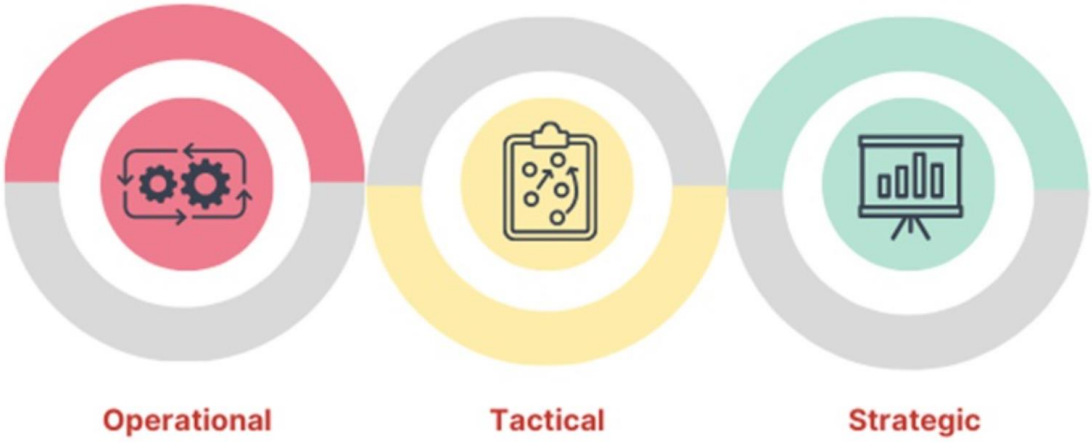

Рис. 2.6. Типи розвідки загроз

Оперативний рівень: якщо корпоративні вимоги до розвідданих полягають у боротьбі з фішинговими кампаніями, що тривають, організація буде прагнути зосередити свої зусилля на зборі оперативних розвідданих. Команда безпеки може використовувати ці дані для блокування IOC за допомогою рішення SIEM або EDR, виявлення сигнатур шкідливого ПЗ за допомогою правил YARA або виявлення шаблонів атак за допомогою правил Sigma.

Тактичний рівень: якщо вимоги організації до розвідданих полягають у визначенні технічних засобів контролю безпеки, які виявлять ISO-файли, що використовуються як початковий вектор доступу, їй потрібно зібрати тактичні розвіддані. Корпоративна команда безпеки буде використовувати ці розвіддані для інженерії виявлення, де вони застосовують встановлені тактики, методи і процедури (TTP) для створення правил виявлення для корпоративного рішення SIEM або EDR.

Стратегічний рівень: якщо вимоги компанії до розвідданих зосереджені на виявленні тенденцій розвитку програм-вимагачів, їй потрібно збирати стратегічні розвіддані, які дають загальне уявлення про те, що відбувається в ландшафті загроз, пов'язаних з програмами-вимагачами. Компанія має поставити

і знайти відповіді на такі запитання: які нові програми-вимагачі з'являються, які вразливості вони використовують і як можна найкраще захиститися від нових тенденцій у цій сфері. Ці питання допоможуть сформувати ширшу стратегію корпоративної безпеки.

Другий фактор, який відіграє роль у тому, як організація використовує життєвий цикл розвідки загроз, - це ресурси, які є в її розпорядженні. Це час, людські ресурси та гроші (Рис. 2.7), які вона може витратити на збір, аналіз та обмін розвідданими.

Рис. 2.7. Головні ресурси циклу розвідки загроз

Час - це, мабуть, найважливіший фактор, який впливає на те, як компанія використовує життєвий цикл розвідки загроз. Це обмежуючий фактор для всіх, і пошук способів максимізації часу має вирішальне значення для створення ефективного життєвого циклу розвідки загроз. В ідеалі, усі хотіли б витрачати якомога більше часу на кожну стадію життєвого циклу, але це нереально. Замість цього організації потрібно визначити пріоритетність етапів і автоматизувати діяльність, де це можливо, щоб заощадити час.

Кадри. Кількість персоналу, яку компанія може виділити для процесів CTI, впливатиме на те, як вона буде використовувати життєвий цикл розвідки загроз. Існує не так багато засобів автоматизації або інструментів, що заощаджують час, в які можна інвестувати, щоб вивільнити час для команди аналітиків і максимально ефективно використати обмежені людські ресурси. Щоб врахувати обмеженість людських ресурсів, організації необхідно визначити пріоритети розвідки загроз. Обов'язковим є детальне обговорення з ключовими зацікавленими сторонами пріоритетних вимог до розвідки загроз, формулювання очікуваних результатів і планування дій.

Гроші - це ключовий фактор для всіх команд безпеки в умовах обмежених ресурсів. Однак, не слід піддаватися спокусі отримати найновіший і найкращий інструмент розвідки. Адже сьогодні в Інтернеті існує безліч ресурсів для збирання інформації, рішень з відкритим вихідним кодом для її зберігання, а також інструментів для аналізу цієї інформації та перетворення її на розвіддані. Також прийнятним варіантом може бути придбання розвідданих у інших компаній за доступні гроші. У таких випадках дешевше буде купити розвіддані у постачальника, ніж витрачати час на створення власних інструментів, які будуть інтегруватися в робочий процес корпоративної команди CTI.

Висновки до розділу 2

Встановлено, що розвідка кіберзагроз (Cyber Threat Intelligence, CTI) діє як проактивний захід безпеки, запобігає витоку даних і зменшує фінансові витрати на відновлення після інцидентів. Завданнями розвідки загроз є збір, аналіз і обробка інформації про потенційні загрози для інформаційної безпеки компанії.

Життєвий цикл розвідки загроз складається з таких етапів: планування (визначення зацікавлених сторін, потреб організації в розвідданих, сфери застосування й основних цілей, пріоритетних об’єктів захисту); збір даних із обраних внутрішніх і зовнішніх джерел; обробка даних (очищення, нормалізація, перевірка законності й достовірності даних); аналіз інформації (інтерпретація даних, виявлення закономірностей і тенденцій, усвідомлення характеру, масштабу й наслідків загроз); поширення інформації серед зацікавлених сторін; зворотний зв’язок від зацікавлених сторін щодо використання розвідувальних даних.

У результаті дослідження з’ясовано, що розвідка загроз збирає дані з багатьох внутрішніх і зовнішніх джерел, які, надають різні види інформації, що доповнюють один одного для створення повної картини загроз. Внутрішні джерела охоплюють системні й мережеві журнали, профілі використання мережі та трафіку, граничні пристрої безпеки, антивірусні системи, дані криміналістики, персонал. До зовнішніх розвідданих відносять дані з загальнодоступних джерел

з відкритим кодом (OSINT), каналів новин, сповіщень, постачальників антивірусів, бази даних уразливостей, порталів безпеки тощо.

Виділяють три типи розвідки загроз: оперативну, тактичну і стратегічну. Оперативна розвідка загроз спрямована на неочікувані й існуючі ризики, зусилля щодо виявлення і реагування на які необхідно пріоритезувати. Тактична розвідка загроз пов'язана з технічними деталями конкретних загроз, таких як вразливості та експлойти. Стратегічна розвідка загроз надає високорівневий огляд ландшафту загроз для формування ширших стратегій безпеки і пріоритезації в розподілі ресурсів.

Розділ 3 ПРАКТИЧНІ АСПЕКТИ ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ РОЗВІДКИ ЗАГРОЗ НА ПІДПРИЄМСТВІ

Зміни у ландшафті зовнішніх і внутрішніх загроз кібербезпеці підприємства створюють нові виклики, які необхідно вирішувати з використанням новітніх технологій захисту інформації. Розвідка загроз, як відзначалося вище, дозволяє виявити й запобігти реалізації кіберзагроз, а отже, зменшити ризики для інформаційних активів, забезпечити стійкість корпоративної системи кіберзахисту і зберегти конкурентоспроможність підприємства на ринку.

Слід відзначити, що використання технологій розвідки загроз на підприємствах та в організаціях різних сфер має свої особливості. Розглянемо приклади типових загроз безпеці підприємства у сферах державного управління, освіти й охорони здоров’я, котрі, як свідчить статистика, все частіше стають мішенями кібератак і потребують впровадження проактивного підходу до кібербезпеки.

3.1 Приклади загроз інформаційній безпеці в компаніях різних галузей

Державний сектор дедалі більше покладається на цифрові технології, що поряд з перевагами наражає установи цієї сфери на додаткові ризики, зважаючи на постійну загрозу кіберзлочинності. Державні органи, заклади охорони здоров'я, університети й державні служби є головними об’єктами для хакерів, які зацікавлені в порушенні роботи критичної інфраструктури.

Нещодавні висновки Європейського агентства з кібербезпеки ENISA [23] наголошують, що основними цілями кібератак є вразливості державного сектору, особливо в урядах та органах державного управління. Цей сектор очолює список найбільш вразливих сфер, на який припадає 24% атак.

Погіршують ситуацію обсяги фінансових втрат внаслідок кіберзагроз. Згідно зі звітом IBM [24], вартість кожного інциденту кібербезпеки в державному секторі в середньому становить 2,6 мільйона доларів США. Варто відзначити, що вартість витоку даних охоплює не лише витрати на усунення наслідків інциденту, але й виплати викупу та судові витрати, які є вагомим тягарем для державних і місцевих бюджетів, призначених для задоволення суспільних потреб. Додатковим ускладнюючим чинником є те, що кіберзлочинці постійно розвиваються і шукають нові шляхи для обходу заходів кібербезпеки.

Кіберзлочинці не випадково обирають публічний сектор своєю мішенню. Основними причинами такого вибору є отримання доступу до великого обсягу даних і привабливість публічного розголосу. Державним установам і організаціям довірено велику кількість конфіденційних і цінних даних, включаючи дані про громадян, урядові операції та інформацію про критично важливу інфраструктуру. Така широта і глибина інформації за своєю суттю приваблює кіберзлочинців, які прагнуть використати її для отримання вигоди.

Оскільки державний сектор контролює критично важливу інфраструктуру громадського транспорту, охорони здоров'я та освіти, потенційна шкода від використання даних є дуже високою. Облікові дані для входу, особисті електронні адреси, адреси, ідентифікаційна інформація, платіжні реквізити тощо можуть бути скомпрометовані, якщо заходи кібербезпеки не спрацюють.

Незважаючи на те, що організації державного сектору намагаються йти в ногу з останніми технологічними тенденціями й удосконалювати заходи кібербезпеки, вони нерідко використовують застарілі IT-системи та програмне забезпечення з уразливостями, які добре відомі кіберзлочинцям. Відсутність нових засобів із розширеними функціями безпеки, а також взаємопов'язаність існуючих систем захисту ставить інформаційні активи державних установ під загрозу кібернападів. Порушення в одному відомстві потенційно може поширитися на інші відомства і системи, створюючи каскадний ефект.

На відміну від приватних компаній з більшими бюджетами, багато організацій державного сектору не повністю готові до захисту від кібератак,

особливо в найбільш схильних до ризику департаментах безпеки, фінансів та IT. Значна залежність державного сектору від коштів платників податків призводить до бюджетних обмежень і бюрократичної тяганини, що, в свою чергу, ускладнює впровадження комплексних заходів кібербезпеки, які відповідають рівню ризику.

Звіт ICMA за 2021 рік [25] показав, що трьома основними перешкодами для кібербезпеки органів місцевого самоврядування є неспроможність платити конкурентоспроможну заробітну плату фахівцям з кібербезпеки, недостатня кількість персоналу з кібербезпеки й загальна нестача коштів на цю важливу сферу.

Організації державного сектору обробляють величезні обсяги конфіденційної інформації - від персональних даних громадян до секретних даних національної безпеки, а довіра громадськості до цих установ означає, що будь-яке порушення безпеки може призвести до масштабних наслідків і громадського розголосу. Кіберзлочинців мотивує можливість порушити роботу, викрасти цінні дані або підірвати довіру громадськості й таким чином здобути популярність, спричинити політичні заворушення й у власних корисливих цілях використати страх і невпевненість серед громадськості.

Порушення роботи або проникнення в організації державного сектору може мати глибокі геополітичні наслідки, дозволяючи кіберзлочинцям чинити тиск, отримувати стратегічні переваги та просувати свої політичні й військові цілі. Наприклад, компрометуючи критично важливу інфраструктуру і викрадаючи конфіденційну інформацію, кіберзлочинці можуть дестабілізувати уряди, підірвати довіру громадськості і маніпулювати міжнародними відносинами. Яскравим прикладом цього став значний сплеск кібератак після початку конфлікту в Україні [26].

Державний сектор є цінною мішенню для кіберзлочинців, які прагнуть використати вразливості для отримання геополітичної вигоди, що робить його основним полем битви на складній арені кібервійни та хакерських атак, що спонсоруються державою.

Основними видами кіберзагроз, що найчастіше спрямовані на державний сектор, є програми-вимагачі, атаки на державний сектор, фішинг, DDoS-атаки, хактивізм [27] (Рис. 3.1).

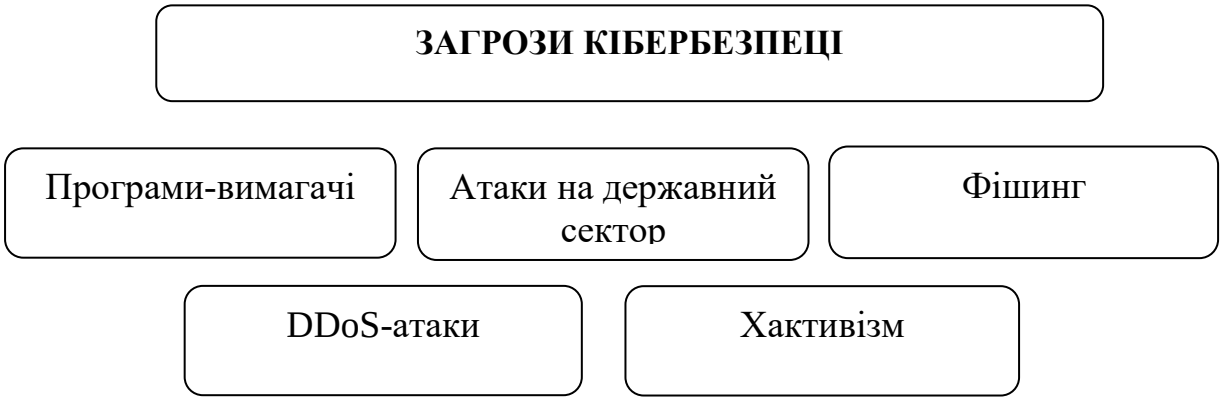

Рис. 3.1. Основні види кіберзагроз державному сектору

Розуміння цих загроз має вирішальне значення для посилення кібербезпеки та захисту цінних активів.

Розглянемо кілька прикладів кібератак на організації державного сектору, зокрема сфери освіти й охорони здоров'я, які мали широкий суспільний резонанс.

На початку 2021 року російський злочинний синдикат здійснив скоординовану атаку з вимогою викупу на понад 20 муніципалітетів Техасу [28]. Безпосереднім наслідком було те, порядок денний засідань і записи актів цивільного стану були недоступні в Інтернеті, однак основні проблеми полягали в тому, що поліція не мала змоги використовувати шукати цифрові записи, а муніципалітети не могли обробляти платіжні відомості. А керівництво одного з міст, які стали жертвами атаки, протягом тижня змушене було керувати системою водопостачання вручну.

Школи борються зі складними кіберзлочинами

У липні 2023 року кенійський портал eCitizen [29] вийшов з ладу після кібератаки, внаслідок якої понад 5 тисяч державних послуг більше не були доступні онлайн. Громадяни не могли отримати доступ до паспортних заявок, гостьових віз, водійських прав, ідентифікаційних карток або медичних записів, а мобільний банкінг і транспортні послуги не працювали. Відповідальність за цей

кіберзлочин взяла на себе група суданських кібервійськових «Анонімний Судан», погрожуючи, що кожен, хто втручатиметься у внутрішні справи Судану, стане мішенню.

Заклади освіти часто зазнають кібератак, які здійснюють хакери з метою отримати доступ до величезної кількості даних та впливу. Об'єднаний шкільний округ Лос-Анджелеса, другий за величиною шкільний округ США, сильно постраждав від хакерських атак на початку 2022/23 навчального року. Російський злочинний синдикат Vice Society [30] зажадав від шкільного округу викуп за викрадення 500 гігабайт конфіденційних даних. Відмова округу сплатити викуп призвела до того, що дані 2 тисяч учнів опинилися в даркнеті, включаючи оцінки, водійські права, номери соціального страхування й результати тестів на COVID.

Всього через кілька місяців ті ж хакери націлилися на освітній сектор Великобританії: 14 шкіл постраждали від спроби вимагання викупу [31] після того, як особиста інформація учнів, включаючи скановані копії паспортів, і контракти працівників були викрадені й викладені в Інтернет. Хакери змусили постраждалі школи виступити з публічними заявами, намагаючись запевнити сім'ї, що їхні дані захищені. Такі атаки відволікають увагу від навчання і змушують адміністрацію шкіл шукати рішення, які зазвичай надходять занадто пізно.

Сфера охорони здоров'я також регулярно стає жертвою хакерських атак. Медичні організації зазнають впливу кіберзлочинності, оскільки володіють величезним обсягом конфіденційної особистої інформації. Атака вірусу-здирника у 2021 році [32] вивела з ладу лікарню St. Margaret's Health у Спрінг-Веллі, штат Іллінойс, що унеможливило подачу страхових відшкодувань пацієнтам протягом декількох місяців. Фінансові труднощі призвели до закриття лікарні у червні 2023 року.

Атаки на медичні установи є частиною тривожної тенденції, оскільки кіберзлочинці йдуть слідами хакерів-здирників WannaCry 2017 року, які здійснили успішну атаку на користувачів Microsoft Windows по всьому світу.

Національна служба охорони здоров'я Великої Британії (NHS) стала однією з найбільших жертв атаки, коли по всій Англії та Шотландії [33] було виведено з ладу до 70 тисяч комп'ютерів і медичних пристроїв. Деяким службам довелося перенаправляти машини швидкої допомоги і відправляти некритичних пацієнтів додому. Загальні втрати Національної служби охорони здоров'я склали 92 мільйони фунтів стерлінгів [34], включаючи значні збитки від скасованих послуг і зусиль для відновлення ІТ.

Типові заходи запобігання і протидії кіберзагрозам, покликані захистити організації державного сектору від невпинної еволюції кіберзагроз і підвищити стійкість критично важливих систем, охоплюють:

1. *Тренінги з підвищення обізнаності про безпеку*: всі співробітники мають проходити регулярне навчання щодо важливості кібербезпеки, актуальних загроз і найкращих практик захисту з використанням реальних прикладів і проведення симуляцій. Заходи навчання й підвищення обізнаності мають відповідати ролі й повноваженням працівника або підрозділу у системі захисту даних організації.

2. *Багатофакторна автентифікація (MFA)*: обов’язковим є впровадження MFA [35] у всіх системах, особливо для привілейованих облікових записів. Цей додатковий рівень безпеки гарантує, що навіть якщо облікові дані будуть скомпрометовані, можна ефективно запобігти несанкціонованому доступу.

3. *Захист кінцевих точок*: важливим завданням є використання передових платформ захисту кінцевих точок, які перевершують традиційні антивірусні рішення. Ці платформи забезпечують моніторинг у режимі реального часу, виявлення загроз та автоматичне реагування на підозрілі дії.

4. *Сегментація мережі*: ізоляція конфіденційних даних шляхом сегментації мережі є запобіжним заходом, який гарантує, що навіть якщо зловмисники отримають доступ до частини мережі, доступ до критично важливих систем або даних стане для них серйозною проблемою.

5. *Регулярні виправлення та оновлення*: підтримувати безпеку всіх систем, додатків і пристроїв, регулярно оновлювати їх найновішими патчами безпеки є

обов’язковим елементом процесу захисту даних, а автоматизовані рішення для управління виправленнями можуть ефективно оптимізувати цей процес.

6. *План реагування на інциденти*: розробка й постійне оновлення комплексного плану реагування на інциденти дозволяє мати актуальні й ефективні процедури реагування, а також забезпечити швидку й адекватну відповідь на події кібербезпеки. Слід регулярно проводити навчання, щоб переконатися, що всі зацікавлені сторони ознайомлені зі своїми ролями та обов'язками у випадку інциденту.

7. *Резервне копіювання та аварійне відновлення*: організації необхідно регулярно створювати резервні копії критично важливих даних і систем, зберігаючи резервні копії як в офісі, так і за його межами. Регулярне тестування процесу відновлення забезпечує цілісність і доступність даних.

8. *Архітектура нульової довіри*: доцільно використовувати архітектуру нульової довіри, де кожен запит на доступ проходить ретельну перевірку, незалежно від його походження. Такий підхід зводить до мінімуму ймовірність внутрішніх загроз і порушень, пов'язаних зі скомпрометованими обліковими даними.

9. *Постійна оцінка вразливостей*: регулярне оцінювання вразливостей і тестування на проникнення забезпечить вчасне виявлення слабких місць у корпоративних системах і додатках. Щоб підтримувати надійний захист виявлені вразливості мають бути негайно усунуті.

10. *Співпраця та обмін інформацією*: Обмін розвідданими про загрози та кращими практиками з усіма зацікавленими сторонами, в томі числі державними установами й наглядовими організаціями, дозволить забезпечити раннє попередження та сприяти колективному захисту від поширених і нових загроз.

3.2 Технології розвідки загроз: застосування і функції

Враховуючи динамічне цифрове середовище, сучасним організаціям важко йти в ногу з розвитком галузі кібербезпеки. Особливої уваги вимагають

нещодавно виявлені вразливості, нові методи атак, а також тактика, прийоми та процедури (TTPs), що використовуються кіберзлочинцями. Як результат, стає все важче знайти джерела й інструменти для вирішення цих трудомістких завдань та отримання корисної інформації.

Огляд ринку засобів розвідки загроз безпеки засвідчив наявність великої кількості інструментів, які будуть корисними на різних етапах розвідувального циклу. Ці інструменти не є універсальними рішеннями, але вони полегшують автоматизований збір, зберігання, обмін та аналіз даних про загрози безпеці й сумісні з іншими рішеннями кібербезпеки. Для формування уявлення про технологічні можливості щодо розвідки загроз, які доступні на ринку, коротко розглянемо найбільш популярні рішення та їх функціонал.

AlienVault Open Threat Exchange

AlienVault Open Threat Exchange [36] (OTX) надає відкритий доступ до глобальної спільноти дослідників загроз і фахівців в галузі безпеки (Рис. 3.2). Рішення надає дані про загрози, створені спільнотою, полегшує спільні дослідження й автоматизує процес оновлення інфраструктури безпеки даними про загрози з будь-якого джерела.

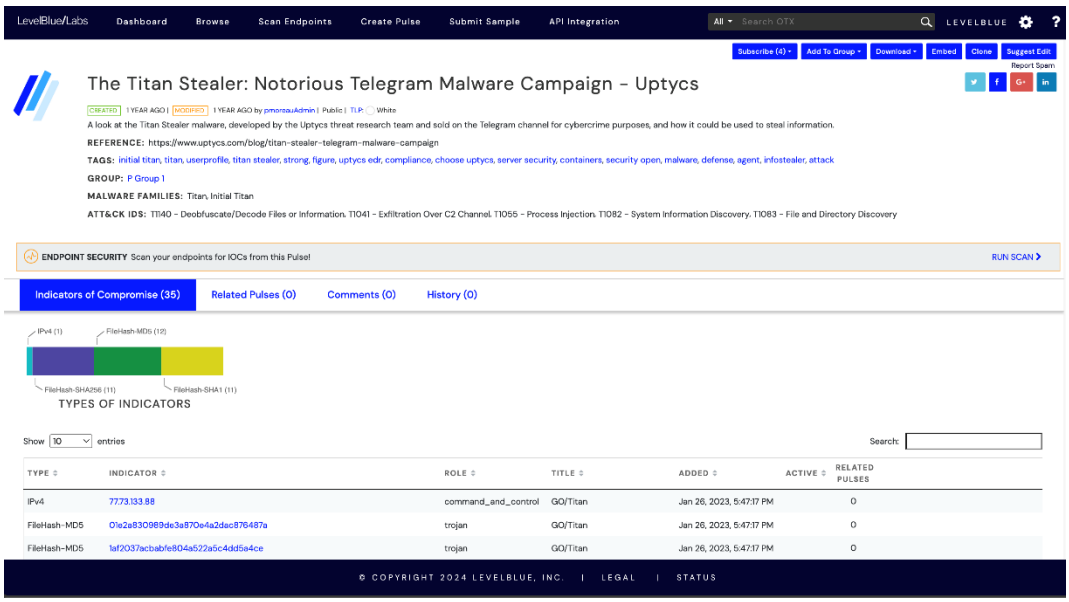

Рис. 3.2. Інтерфейс платформи AlienVault

Платформа служить оригінальним краудсорсинговим джерелом даних про загрози і є однією з найкращих для щоденної обробки понад 1900 мільйонів

нових записів про порушення (IoC). Ця платформа легка у використанні й надає аналітичні дані про загрози в різних форматах, включаючи STIX, OpenIOC, MAEC, JSON та CSV. Кожна відправлена вибірка називається "pulse".

Отримання певних, попередньо відфільтрованих даних дозволяє гнучко визначати конкретні вимоги. Також є можливість отримувати канали, адаптовані до типів пристроїв, таких як кінцеві точки. Якщо відповідні дані не входять в параметри каналу, ці додаткові дані прив'язуються до наданого запису. Політика безпеки є незамінним інструментом для будь-якої програми інформаційної безпеки, але вона не може жити у вакуумі. Щоб забезпечити комплексний захист від загроз і усунути вразливості, легко проходити аудит безпеки та швидко відновлюватися після інцидентів, важливо використовувати як адміністративні, так і технічні засоби контролю.

Важливо також, щоб платформа добре розуміла, які зловмисники можуть націлитися на важливі корпоративні дані, на яких тактиках, методах і процедурах слід зосередитися і які дії слід вжити. Деякі приклади платформ та інструментів для розвідки загроз для малого, середнього та великого бізнесу наведені нижче.

CTI4SOC

CTI SOCRadar, CTI4SOC [37] є платформою аналізу загроз нового покоління, призначеною для полегшення роботи аналітиків SOC. Вона служить унікальним помічником для команди SOC завдяки 12 функціональним модулям.

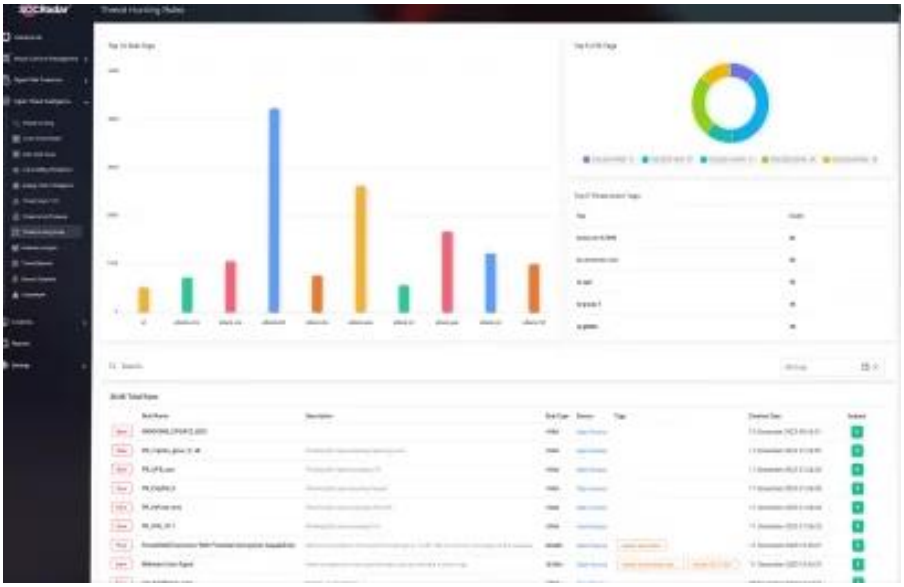

Рис. 3.3. Інтерфейс платформи CTI4SOC

На відміну від традиційних платформ аналізу загроз, CTI4SOC використовує великі дані для організованого і контекстуального представлення всіх даних, які аналітики можуть отримати за допомогою різних інструментів. Платформа відбирає та фільтрує інформацію з точки зору аналітиків і надає правильні гіпотези для початку дослідження загроз конкретної організації. CTI4SOC не тільки збирає корисну інформацію, але й представляє її в практичному контексті. Вона надає доступ в один клік до звітів про загрози, що публікуються аналітиками безпеки SOCRadar та іншими надійними джерелами.

Розуміння аналітиками SOC тактики, методів, процедур (TTPs), мотивацій і моделей поведінки цих зловмисників допомагає сформувати обґрунтовану точку зору, використовуючи CTI4SOC для додавання активних учасників загроз в список моніторингу та відстеження їх дій.

Рис. 3.4. Відображення аналітичних даних у CTI4SOC

Модуль пошуку загроз SOCRadar [38] є найціннішим інструментом для аналітиків SOC після завершення етапу досліджень. З його допомогою фахівці служби безпеки можуть розширити свою роботу, шукаючи важливу інформацію про центри управління (C2), зловмисне ПЗ, IP-адреси та домени. CTI4SOC-це

рішення з підтримкою API, яке робить усі ці корисні дані легко доступними у разі потенційної атаки.

DOCGuard

DOCGuard - це служба аналізу шкідливих програм, яка інтегрується з рішеннями Secure Email Gateways (SEGs) та SOAR [39].

Служба використовує новий тип статичного аналізу, який називається структурним аналізом. Таким чином, шкідливе ПЗ фрагментується й переноситься в ядро на основі компонентів файлової структури. Застосовуючи цей підхід, DOCGuard може чітко виявляти шкідливі програми, витягувати індикатори порушення без помилкових спрацьовувань (false positive free) (IoC), виявляти шифрування у вигляді послідовного кодування і шифрування документів.

У даний час підтримуються такі типи файлів, як файли Microsoft Office, PDF, HTML, HTMs, LNKs, JScript, ISO, IMG, VHD, VCF та архіви (zip, rar тощо). Детальні результати структурного аналізу відображаються у зведеному поданні графічного інтерфейсу користувача та можуть бути завантажені у вигляді звіту у форматі JSON. Ці результати також можна отримати за допомогою API.

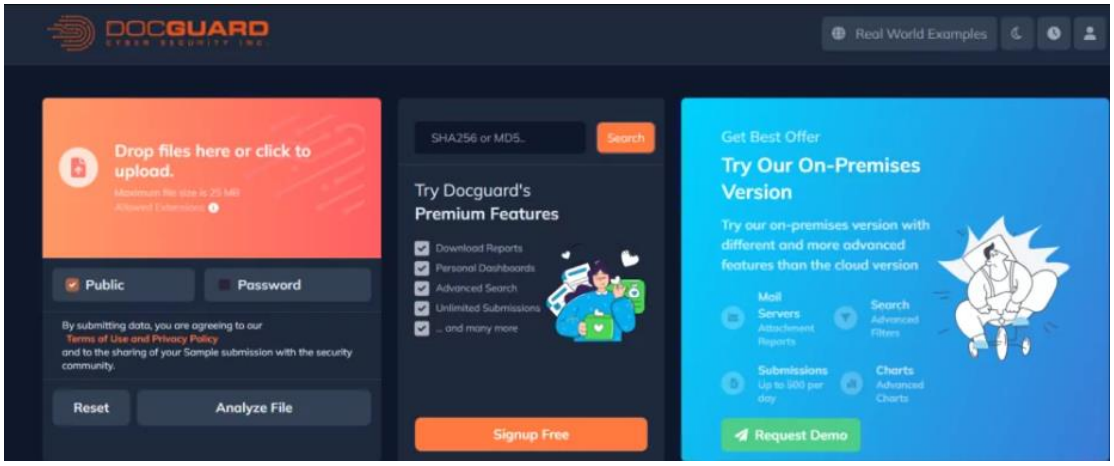

Рис. 3.5. Інтерфейс сервісу DOCGuard

Сервіс забезпечує швидкий вибірковий аналіз і легко інтегрується в екосистему кібербезпеки за лічені хвилини за допомогою інтерфейсу API.

GreyNoise

GreyNoise [40] забезпечує наочність і глибокий контекст для аналітиків розвідки загроз і мисливців за загрозами. Він збирає й аналізує дані про активність користувачів в Інтернеті, щоб допомогти зменшити кількість помилкових спрацьовувань при аналізі інформації про загрози. GreyNoise збирає інформацію про шкідливі сканери, такі як Shodan [41], а також про зловмисників, таких як SSH-хробаки та Telnet-хробаки, визначає дані про шум, які можуть бути відсутні в аналітиків SOC.

GreyNoise визначає інтернет-браузери і звичайні бізнес-операції в подіях безпеки, що дозволяє приймати більш швидкі й безпечні рішення. Незалежно від того, чи аналітик використовує переглядач, API або інтегрує дані GreyNoise у засоби безпеки, він може знайти щось важливе в журналі безпеки й повернутися до роботи.

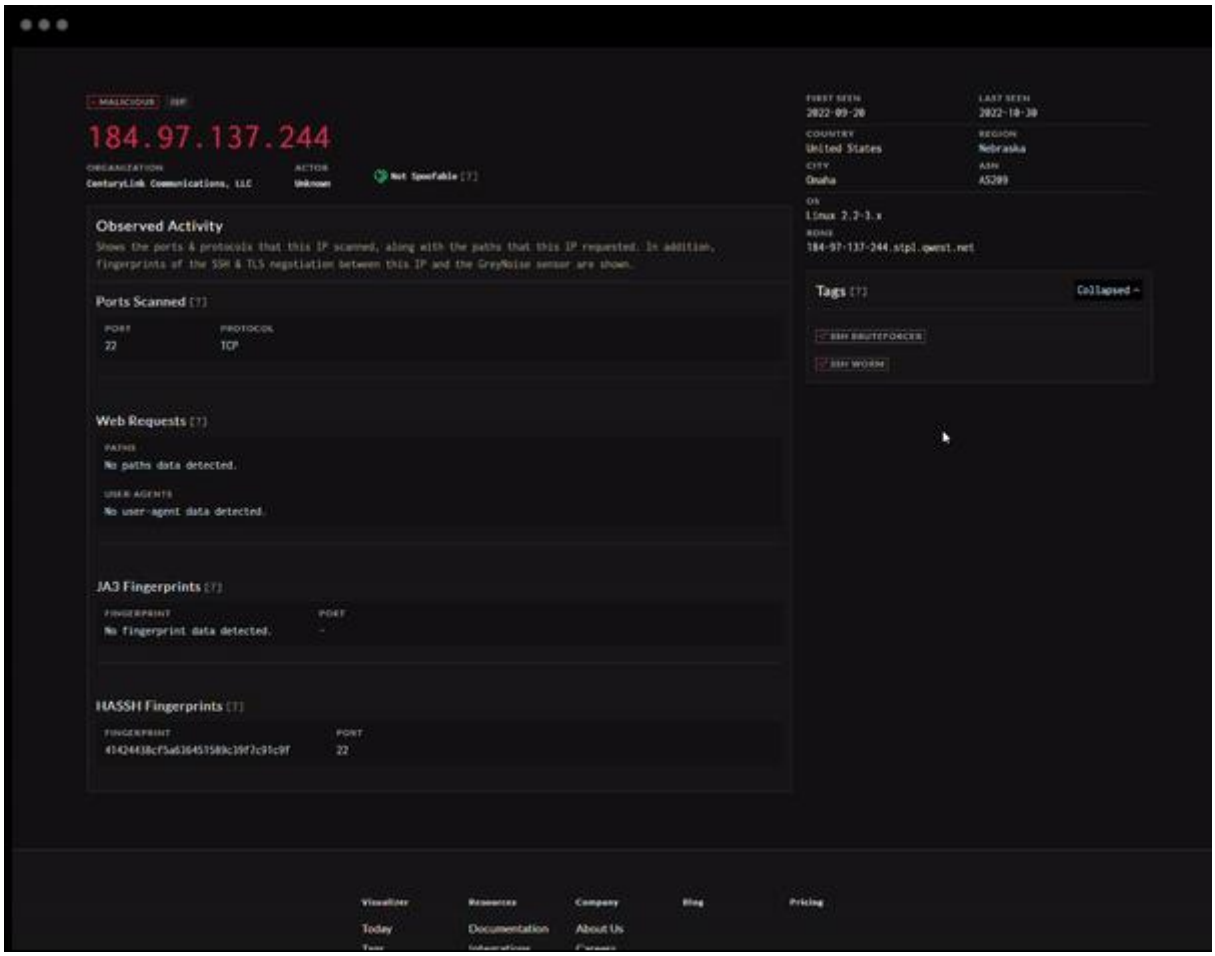

Рис. 3.6. Інтерфейс сервісу GreyNoise

Інтеграція GreyNoise спрощує роботу з даними платформи Threat Intelligence Platform (TIP) і допомагає усунути шум і помилкові спрацьовування,

з якими команди розвідки загроз, зазвичай, стикаються при роботі з різними джерелами розвідувальної інформації. Пошук загроз дозволяє GreyNoise ідентифікувати незвичайні тактичні схеми, методи та процедури (TTPs), тим самим виявляючи кампанії та інфраструктуру противника. Також інструментом аналізу GreyNoise можна скористатися для більш глибокого вивчення показників порушень (IoCs), щоб прискорити терміни розслідування.

Intezer

Intezer - це платформа, призначена для аналізу й перевірки попереджень, та створена для таких як досвідчені аналітики безпеки та реінжинірингові компанії [42].

Самоорієнтована SOC платформа Intezer визначає пріоритети сповіщень і досліджує загрози для корпоративної команди в режимі 24/7. Використовуючи автоматичний аналіз, інтелектуальні рекомендації й автоматичне виправлення помилок, Intezer позбавляє команду SOC від витрачання часу на обробку помилкових спрацьовувань, повторюваних завдань аналізу і занадто великої кількості високорівневих і трудомістких попереджень.

Intezer Analyze - це універсальна платформа для аналізу шкідливих програм, яка може виконувати статичний, динамічний і генетичний аналіз коду всіх типів файлів [43]. Це дозволяє командам реагування на інциденти та SOC оптимізувати розслідування інцидентів, пов'язаних із шкідливим ПЗ. Користувачі можуть відстежувати сімейства шкідливих програм, витягувати IoCs/MITRE TTPs і завантажувати підписи YARA.

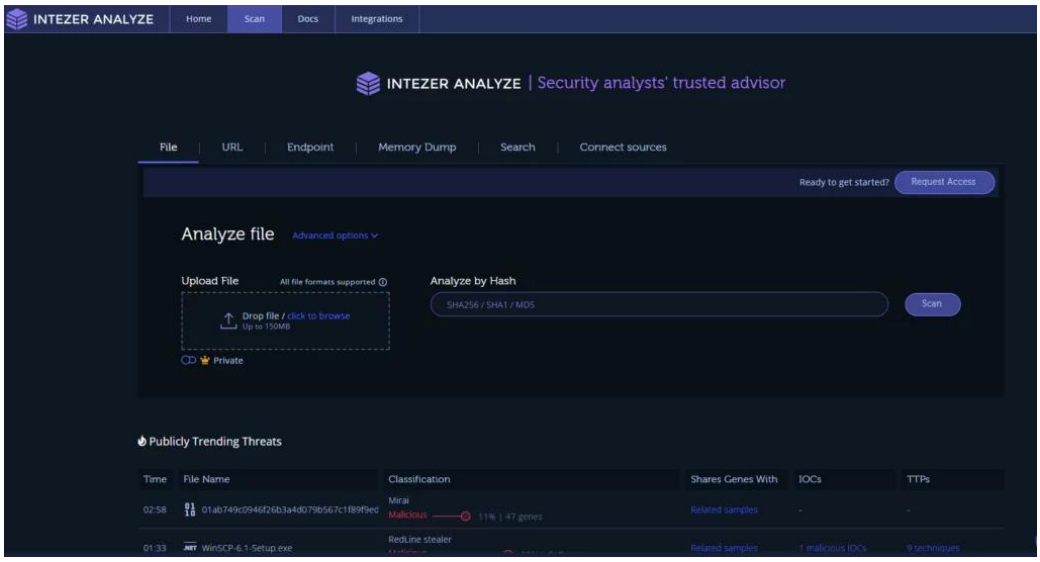

Рис. 3.7. Інтерфейс платформи Intezer Analyze

За допомогою Intezer Transformations аналітики зловмисного ПЗ і дослідники загроз можуть швидко отримувати відповіді про підозрілі файли й кінцеві точки, класифікувати підозрілі файли та комп'ютери за лічені секунди, скоротити час відгуку й об'єднати кілька засобів аналізу шкідливих програм в один.

Дана платформа дозволяє створювати своєчасні та детальні звіти, завантажувати потенційно конфіденційні дані й автоматично визначати пріоритети, а також перевіряти всі сповіщення, надаючи інформацію лише про підтверджені й серйозні загрози.

MISP Threat Sharing

MISP, раніше відома як платформа обміну інформацією про зловмисне ПЗ, - це безкоштовна платформа аналізу загроз із відкритим кодом та відкритими стандартами для обміну інформацією про загрози. Створена службою комп’ютерної безпеки CIRCL [44], вона виконує функції збору, зберігання, поширення й обміну інформацією про загрози й інциденти кібербезпеки, а також аналізу шкідливих програм.

MISP розроблений аналітиками SOC, експертами з безпеки та ІКТ, а також інженерами з аналізу шкідливих програм для підтримки повсякденних операцій та ефективного обміну структурованою інформацією. У міру розширення проекту MISP [45] він охоплював не лише показники зловмисного ПЗ, а й

інформацію про шахрайство та вразливості. На даний час MISP - це проект спільноти, який очолює команда волонтерів.

Мета MISP - полегшити обмін структурованою інформацією всередині спільноти безпеки та за її межами. MISP надає можливості для підтримки обміну та використання інформації системою виявлення мережевих вторгнень (NIDS), LIDS та SIEM, інструментом аналізу журналів.

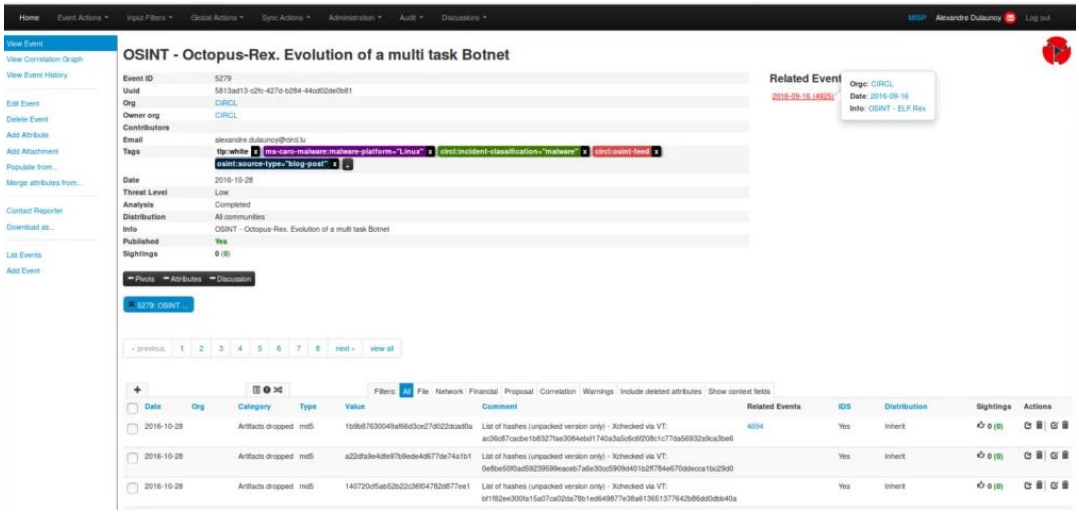

Рис. 3.8. Інтерфейс платформи MISP

Ключовими особливостями платформи MISP є:

- Ефективна база даних IoCs і показників, в якій може зберігатися технічна і нетехнічна інформація про зразки шкідливих програм, інциденти, зловмисників і аналітичних даних.
- Автоматична кореляція для пошуку взаємозв'язків між атрибутами й показниками шкідливих програм, кампаній проти атак або аналітики.
- Гнучка модель даних, яка може представляти і пов'язувати складні об'єкти, а також інформацію про загрози, події чи пов'язані елементи.
- Вбудовані можливості спільного використання, які полегшують обмін даними за допомогою різних моделей розповсюдження.
- Інтуїтивно зрозумілий користувальницький інтерфейс, що дозволяє кінцевим користувачам створювати, оновлювати події та атрибути / індикатори та співпрацювати.

- Гнучкий API для інтеграції MISP з власними рішеннями відповідно до потреб конкретної організації.
- MISP постачається з PyMISP - гнучкою бібліотекою Python для доступу до платформи MISP через REST API. Це дозволяє отримувати події, додавати або оновлювати події/атрибути, додавати або оновлювати зразки шкідливих програм і шукати атрибути.
- Інтелектуальний словник під назвою MISP GALAXY включає існуючі джерела загроз, зловмисне ПЗ, RAT, програми-вимагачі та Mitre ATT&CK, які можна легко пов'язати з подіями та атрибутами MISP.

Знання поширених інструментів розвідки загроз є важливим для визначення потреб і заходів щодо забезпечення безпеки корпоративної IT-інфраструктури та зменшення ризиків кібербезпеки. Фахівці з аналізу загроз мають пройти відповідну підготовку і набути навичок, необхідних для застосування правильних методів забезпечення безпеки.

3.3 Рекомендації щодо впровадження розвідки загроз на підприємстві

Аналітика загроз використовує інструменти та методології для аналізу даних, які допомагають зменшити ризики та виявити існуючі або виникаючі загрози безпеці організації. Аналітика загроз допомагає організаціям приймати більш швидкі та обґрунтовані рішення щодо безпеки та заздалегідь змінювати поведінку з реактивної на проактивну для протидії атакам.

Одним із найбільших викликів сьогодення є осмислення всієї інформації про загрози, яку організації отримують з різних джерел: комерційних і відкритих, від уряду, галузевих торговельних груп і постачальників систем безпеки.

Дослідження ролі розвідки загроз показало, що при виборі і впровадженні засобів розвідки загроз на підприємстві доцільно дотримуватися таких рекомендацій:

Вибір правильних джерел даних про загрози

Не всі дані про загрози однакові, і вони можуть значно відрізнятися в різних компаніях. Тому цінність даних зводиться до релевантності й доступності, що вимагає вибору індивідуального джерела отримання й агрегування даних, відфільтрованих за різними чинниками, такими як географія, галузь, інфраструктура, профіль ризику тощо.

Починаючи з внутрішніх даних, подій і телеметрії, доповнюючи їх зовнішніми даними для контекстуалізації інформації з внутрішніх систем, можна зрозуміти релевантність і зосередитися на тому, що є пріоритетним для кожної компанії.

Визначення того, хто буде отримувати дані

Хоча надання доступу до даних про загрози широкій аудиторії може бути цілком виправданим, краще мати команду, відповідальну за збір і аналіз розвідданих про загрози, і надавати тільки ту інформацію, яка може бути використана для конкретних дій.

Не всі зацікавлені сторони потребують доступу до максимальних розвідданих, тому слід прорахувати, як один і той самий звіт вплине на різні команди в компанії (стратегічні, оперативні, тактичні) і як він буде ними використовуватися.

Структурування даних для аналізу

Дані про загрози надходять у різних форматах і потребують стандартизації. Обсяг інформації у сфері розвідки загроз великий і має різні назви. Процес, який дозволяє швидко агрегувати й організовувати інформацію називається *нормалізацією*. Інтелектуальна платформа автоматично отримує і нормалізує дані, структуруючи їх в єдиний спосіб, щоб їх можна було контекстуалізувати і розставити за пріоритетами, допомагаючи зосередитися на найбільш важливих загрозах.

Використання інструментів для аналізу

Аналіз даних є складним, але важливим завданням для будь-якої компанії. Хороша платформа для розвідки загроз витягує контекст і допомагає

використовувати інформацію по-різному для різних сценаріїв, а також підтримує різні результати.

Моніторинг

Основною метою моніторингу безпеки є виявлення загроз, щоб запобігти потенційним порушенням безпеки й підтримувати безпечне середовище. Однак треба розуміти, що не всі загрози можуть бути превентивно заблоковані. У цьому випадку моніторинг також служить механізмом виявлення причини інциденту безпеки, що стався, незважаючи на запобіжні зусилля.

До моніторингу можна підходити з різних точок зору:

- *Моніторинг на різних висотах*. Моніторинг з різних висот - це процес отримання інформації про потоки користувачів, доступ до даних, ідентифікацію, мережі та навіть операційні системи. Кожен з цих рівнів надає унікальну інформацію, яка допомагає виявити відхилення від очікуваної поведінки, встановленої відповідно до базового рівня безпеки. І навпаки, постійний моніторинг систем і додатків протягом певного періоду часу може встановити цей базовий рівень. Наприклад, зазвичай кожну годину в системі ідентифікації може відображатися близько 1000 спроб входу. Якщо моніторинг виявляє сплеск 50 000 спроб входу за короткий проміжок часу, це може свідчити про те, що зловмисник пробує отримати доступ до системи.

- *Моніторинг в різних сферах впливу*. Дуже важливо стежити за додатком і платформою. Припустимо, користувач програми випадково отримав підвищені привілеї або сталося порушення безпеки. Якщо користувач виконує дію, яка перевищує певні рамки, наслідки можуть бути обмежені діями, які виконують інші користувачі. Однак ступінь потенційного збитку, який може бути завданий в разі злому бази даних внутрішньою організацією, не була визначена. Радіус вибуху або масштаб впливу можуть сильно відрізнятися залежно від того, який із цих сценаріїв відбудеться.

- *Використання спеціальних інструментів моніторингу*. Дуже важливо інвестувати в спеціалізовані інструменти, які завжди допоможуть виявити аномальну поведінку, що може свідчити про атаку. Більшість із цих інструментів

мають можливості аналізу загроз на основі великих обсягів даних і відомих загроз, не залежать від стану і містять глибоке розуміння телеметрії в контексті безпеки. Щоб отримувати детальні сигнали від платформи й робити прогнози з високою точністю, інструмент має бути інтегрований або, принаймні, орієнтований на платформу, мати змогу генерувати своєчасні повідомлення з достатньою кількістю інформації для правильного сортування. Використання занадто великої кількості різних інструментів може призвести до ускладнення.

- *Використання моніторингу для реагування на інциденти*. Перетворення агрегованих даних в оперативну розвідувальну інформацію забезпечує швидке й ефективне реагування на інциденти. У цьому контексті мета моніторингу полягає в зборі достатньої кількості даних для аналізу і розуміння події, щоб у подальшому вживати належних заходів після інциденту. Моніторинг забезпечує збір даних про минулі події для покращення можливостей реагування і прогнозування майбутніх інцидентів

Тестування безпеки

Ретельне тестування є основою хорошого дизайну системи безпеки. Тестування - це форма тактичної перевірки, що дозволяє переконатися в тому, що засоби управління функціонують правильно. Тестування також є проактивним способом виявлення вразливостей у системі. Для тестування корпоративної платформи та інфраструктури потрібно охопити внутрішню перспективу, а також зовнішню оцінку для тестування системи як зовнішнього зловмисника.

Реагування на інциденти безпеки

Команда виконує операції з реагування на інциденти, коли надходить сигнал або попередження, що вказує на потенційний інцидент безпеки. Високоточні повідомлення містять достатньо інформації про безпеку, щоб полегшити аналітикам прийняття рішень, а також знижують кількість помилкових спрацьовувань. Варто звернути увагу на те, щоб система оповіщення ігнорувала сигнали низької точності і фокусувалася на високоточних повідомленнях, які переважно вказують на реальні інциденти.

Сповіщення про безпеку треба надсилати відповідним користувачам: членам команди безпеки й персоналу компанії. Доцільно визначити контактну особу в робочій групі для отримання повідомлень про інциденти, які мають містити якомога більше інформації про скомпрометовані ресурси й системи.

Рекомендується реєструвати оповіщення та дії з розслідування інцидентів і управляти ними за допомогою спеціалізованих інструментів, які відстежують хід перевірки. Стандартні інструменти дозволяють зберігати будь-які докази, які можуть знадобитися для можливого розслідування. Варто знаходити можливості для автоматизації, яка надсилає сповіщення встановленим відповідальним особам. Під час інциденту слід дотримуватися чіткого ланцюжка взаємодії та звітності.

Також фахівці радять скористатися рішеннями з управління інформацією і подіями безпеки (SIEM) і автоматичного реагування (SOAR). Крім цього, компанія може придбати інструменти управління інцидентами, які допоможуть стандартизувати роботу всіх груп навантаження.

Відновлення після інцидентів

Підприємство має ставитися до кожного інциденту безпеки як до катастрофічного. Якщо для виправлення ситуації потрібне повне відновлення, слід використовувати механізм відновлення, який відповідає вимогам безпеки і дозволяє запобігти можливості повторення. В іншому випадку, при повторному розгортанні системи з такою ж вразливістю відбудеться аналогічний інцидент. Необхідно постійно переглядати процедури і процеси, пов'язані з аварійним завершенням та відновленням після аварії.

Якщо система продовжує працювати, варто оцінити вплив на робочу частину системи, щоб не порушити конфіденційність, зменшити ризики для системи, забезпечити надійність та продуктивність або їх коригування шляхом впровадження відповідних процесів деградації.

Важливим елементом відновлення є діагностика, за результатами якої забезпечується потенційна можливість виправлення та резервного копіювання. Після встановлення діагнозу команда працюватиме над вирішенням ситуації, визначатиме та вноситиме необхідні виправлення протягом встановленого часу.

Показники відновлення визначають, скільки часу знадобиться для вирішення проблеми. Для стабілізації системи потрібен час на виправлення, внесення змін, проведення тестів і розгортання оновлень, визначення стратегій стримування для запобігання подальшої шкоди та поширення інцидентів, розробку процедур усунення загроз із корпоративного середовища.

Висновки до розділу 3

Аналіз випадків реалізації загроз інформаційній безпеці показав, що впродовж останніх років все частіше мішенями кібератак стають підприємства й організації у сферах державного управління, освіти й охорони здоров'я, що свідчить про нагальну необхідність впровадження ними проактивного підходу до кібербезпеки. Типові заходи запобігання і протидії кіберзагрозам, покликані захистити організації публічного сектору від кіберзагроз і підвищити стійкість критично важливих систем, охоплюють: навчання персоналу з питань безпеки, є: багатофакторна автентифікація, захист кінцевих точок, сегментація мережі, регулярні виправлення й оновлення, планування реагування на інциденти, резервне копіювання й аварійне відновлення, використання архітектури нульової довіри, постійна оцінка вразливостей, співпраця та обмін інформацією.

Огляд ринку засобів розвідки загроз безпеки засвідчив наявність великої кількості інструментів, які будуть корисними на різних етапах розвідувального циклу, серед яких безкоштовна платформа розвідувальної спільноти з понад 20 млн індикаторів загроз AlienVault; платформа аналізу загроз нового покоління на основі великих даних CTI4SOC; служба аналізу шкідливих програм DOCGuard; сервіс збирання й аналізу даних про Інтернет-активність користувачів, шкідливі сканери, зловмисні програми GreyNoise; платформа, призначена для аналізу й перевірки попереджень Intezer; безкоштовна платформа аналізу загроз із відкритим кодом і відкритими стандартами для обміну даними про загрози MISP.

Ці інструменти не є універсальними рішеннями, але вони полегшують автоматизований збір, зберігання, обмін та аналіз даних про загрози безпеці й сумісні з іншими рішеннями кібербезпеки.

Дослідження ролі розвідки загроз показало, що при виборі і впровадженні засобів розвідки загроз на підприємстві доцільно дотримуватися низки рекомендацій, зокрема:

Обирати релевантні, доступні, відфільтровані за обраними критеріями дані про загрози.

Надавати доступ до даних про загрози тільки уповноваженим фахівцям для виконання конкретних завдань.

Структурувати дані про загрози для подальшого аналізу шляхом використання інтелектуальних платформ, які автоматично отримують, нормалізують і пріоритезують дані, зосереджуючись на найбільш важливих загрозах.

Використовувати інструменти для аналізу даних про загрози, зокрема моніторинг, який дозволяє не тільки виявляти загрози, щоб запобігти потенційним порушенням безпеки, але й служить механізмом виявлення причин інциденту безпеки, що стався, незважаючи на запобіжні заходи; тестування безпеки, яке є проактивним методом виявлення вразливостей у системі.

Здійснювати реагування на події безпеки на основі сигналів або високоточних попереджень, що містять достатньо інформації і вказують на потенційний інцидент безпеки, знижуючи кількість помилкових спрацьовувань.

Використовувати засоби аналізу загроз у ході відновлення після інцидентів, зокрема, шляхом проведення діагностики, за результатами якої забезпечується виправлення та резервне копіювання, впровадження механізму відновлення, визначення стратегій стримування для запобігання подальшій шкоді й поширенню інцидентів.

ВИСНОВКИ

Дослідження показало, що управління інформаційною безпекою передбачає розроблення, впровадження, функціонування, моніторинг, перегляд, підтримку і вдосконалення інформаційної безпеки організації і реалізується шляхом впровадження комплекс адміністративних, фізичних і технічних заходів.

Встановлено, що розвідка кіберзагроз (Cyber Threat Intelligence, CTI) є важливим елементом управління інформаційною безпекою підприємства і діє як проактивний захід безпеки, запобігає витоку даних і зменшує фінансові витрати на відновлення після інцидентів. Завданнями розвідки загроз є збір, аналіз і обробка інформації про потенційні загрози для інформаційної безпеки компанії.

Життєвий цикл розвідки загроз складається з таких етапів: планування; збір даних із обраних внутрішніх і зовнішніх джерел; обробка даних; аналіз інформації; поширення інформації серед зацікавлених сторін; зворотний зв’язок від зацікавлених сторін щодо використання розвідувальних даних. Розвідка загроз збирає дані з багатьох внутрішніх і зовнішніх джерел, які, надають різні види інформації, що доповнюють один одного для створення повної картини загроз.

Виділяють три типи розвідки загроз: оперативну, тактичну і стратегічну. Оперативна розвідка загроз спрямована на неочікувані й існуючі ризики, зусилля щодо виявлення і реагування на які необхідно пріоритезувати. Тактична розвідка загроз пов'язана з технічними деталями конкретних загроз, таких як вразливості та експлойти. Стратегічна розвідка загроз надає високорівневий огляд ландшафту загроз для формування ширших стратегій безпеки і пріоритезації в розподілі ресурсів.

Огляд ринку засобів розвідки загроз безпеки засвідчив наявність великої кількості інструментів, які будуть корисними на різних етапах розвідувального циклу, серед яких безкоштовна платформа розвідувальної спільноти з понад 20 млн індикаторів загроз AlienVault; платформа аналізу загроз нового покоління на основі великих даних CTI4SOC; служба аналізу шкідливих програм DOCGuard; сервіс збирання й аналізу даних про Інтернет-активність користувачів, шкідливі

сканери, зловмисні програми GreyNoise; платформа, призначена для аналізу й перевірки попереджень Intezer; безкоштовна платформа аналізу загроз із відкритим кодом і відкритими стандартами для обміну даними про загрози MISP.

Ці інструменти не є універсальними рішеннями, але вони полегшують автоматизований збір, зберігання, обмін та аналіз даних про загрози безпеці й сумісні з іншими рішеннями кібербезпеки.

За результатами дослідження запропоновано рекомендації щодо вибору і впровадження засобів розвідки загроз на підприємстві:

Обирати релевантні, доступні, відфільтровані за обраними критеріями дані про загрози.

Надавати доступ до даних про загрози тільки уповноваженим фахівцям для виконання конкретних завдань.

Структурувати дані про загрози для подальшого аналізу шляхом використання інтелектуальних платформ, які автоматично отримують, нормалізують і пріоритезують дані, зосереджуючись на найбільш важливих загрозах.

Використовувати інструменти для аналізу даних про загрози, зокрема моніторинг, який дозволяє не тільки виявляти загрози, щоб запобігти потенційним порушенням безпеки, але й служить механізмом виявлення причин інциденту безпеки, що стався, незважаючи на запобіжні заходи; тестування безпеки, яке є проактивним методом виявлення вразливостей у системі.

Здійснювати реагування на події безпеки на основі сигналів або високоточних попереджень, що містять достатньо інформації і вказують на потенційний інцидент безпеки, знижуючи кількість помилкових спрацьовувань.

Використовувати засоби аналізу загроз у ході відновлення після інцидентів, зокрема, шляхом проведення діагностики, за результатами якої забезпечується виправлення та резервне копіювання, впровадження механізму відновлення, визначення стратегій стримування для запобігання подальшій шкоді й поширенню інцидентів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Хорошко В.О., Чередниченко В.С., Шелест М.Є. Основи інформаційної безпеки / За ред. проф. В.О. Хорошка. К.: ДУІКТ, 2008. 186 с.

2. Information Security: The Ultimate Guide. *Imperva*. URL: https://www.imperva.com/learn/data-security/information-security-infosec/.

3. What is cybersecurity? *IBM.* URL: https://www.ibm.com/topics/cybersecurity.

4. What is cybersecurity? *Cisco*. URL: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html.

5. Cyber security. Governance, Risk Management and Compliance for Information Technology. *IT Governance.* URL: https://www.itgovernance.co.uk/what-is-cybersecurity.

6. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).

7. Горяна О.Г. Система управління інформаційною безпекою. CORE. URL: https://core.ac.uk/download/pdf/48401951.pdf.

8. Cybersecurity threats: types and challenges - exabeam. *Exabeam*. URL: https://www.exabeam.com/information-security/cyber-security-threat/#MITRE.

9. Nearly two thirds of CISOs have had to deal with the loss of sensitive data in the past 12 months. Proofpoint report. *10 Guards*. URL: https://10guards.com/en/articles/nearly-two-thirds-of-cisos-have-had-to-deal-with-the-loss-of-sensitive-data-in-the-past-12-months-proofpoint-report/.

10. 15 тривожних фактів та статистики про кібербезпеку. URL: https://corewin.ua/blog/cybersecurity-facts-and-statistics/.

11. Pharming. *Imperva*. URL: https://www.imperva.com/learn/application-security/pharming/.

12. What is a supply chain attack? Connect, Protect and Build Everywhere. *Cloudflare*. URL: https://www.cloudflare.com/learning/security/what-is-a-supply-chain-attack/.

13. What is bluetooth in cyber security? Understanding bluetooth attacks. *Zenarmor*. URL: https://www.zenarmor.com/docs/network-basics/what-is-bluetooth.

14. Golden ticket. *HackTricks.* URL: https://book.hacktricks.xyz/v/ua/windows-hardening/active-directory-methodology/golden-ticket.

15. What is cybersecurity management? Framework, risks and trends. *Fortinet*. URL: https://www.fortinet.com/resources/cyberglossary/cybersecurity-management

16. Повний посібник з аналізу кіберзагроз. *Софтико*. URL: https://softico.ua/uk/bez-kategoriyi/povnij-posibnik-z-analizu-kiberzagroz/.

17. The cyber threat intelligence lifecycle: a fundamental model. *Kraven Security*. URL: https://kravensecurity.com/the-threat-intelligence-lifecycle/

18. Get to know the 6 stages of the threat intelligence lifecycle. *MemcyCo*. URL: https://www.memcyco.com/home/6-stages-of-the-threat-intelligence-lifecycle/.

19. Applying threat intelligence to star wars. The diamond model. *ThreatConnect*. URL: https://threatconnect.com/blog/diamond-model-threat-intelligence-star-wars/.

20. Cyber kill chain. *GeeksforGeeks*. URL: https://www.geeksforgeeks.org/cyber-kill-chain/.

21. Discover what threat intelligence is. 3 key attributes. *Sumo Logic*. URL: https://www.sumologic.com/glossary/threat-intelligence/.

22. Ramsdale A., Shiaeles S., Kolokotronis N. A Comparative Analysis of Cyber-Threat Intelligence Sources, Formats and Languages. Electronics 9(5), 824. May 2020. DOI:10.3390/electronics9050824

23. Cybersecurity: main and merging theats. *European Parliament*. URL: https://www.europarl.europa.eu/topics/en/article/20220120STO21428/cybersecurity-main-and-emerging-threats.

24. IBM Registration form. *IBM*. URL: https://www.ibm.com/account/reg/us-en/signup?formid=urx-52258.

25. A Look at Local Government Cybersecurity in 2020. *ICMA*. URL: https://icma.org/articles/pm-magazine/look-local-government-cybersecurity-2020.

26. Lyngaas S. Exclusive: US government agencies hit in global cyberattack | CNN Politics. *CNN*. URL: https://edition.cnn.com/2023/06/15/politics/us-government-hit-cybeattack/index.html.

27. What is Hacktivism? *Checkpoint* URL: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-hacktivism/.

28. Cyber-insecurity: Preparing for public sector to better mitigate cyber-risk. *Thomson Reuters Institute*. URL: https://www.thomsonreuters.com/en-us/posts/government/government-agencies-mitigating-cyber-risk/.

29. Mwai P., Nkonge A. Kenya cyber-attack: Why is eCitizen down? *BBC*. URL: https://www.bbc.com/news/world-africa-66337573.

30. Harter C. LAUSD cyberattack far worse than reported, 2,000 students compromised. *Daily News*. 2023. URL: https://www.dailynews.com/2023/02/22/lausd-cyberattack-far-worse-than-reported-with-2000-students-compromised/.

31. Holmes B. J. Schools hit by cyber attack and documents leaked. *BBC*. URL: https://www.bbc.com/news/uk-england-gloucestershire-63637883.

32. Collier K. An Illinois hospital is the first health care facility to link its closing to a ransomware attack. *NBC News*. URL: https://www.nbcnews.com/tech/security/illinois-hospital-links-closure-ransomware-attack-rcna85983.

33. NHS ransomware attack spreads worldwide. *PubMed Central (PMC)*. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5461132/.

34. WannaCry cyber-attack cost the NHS £92m after 19,000 appointments were cancelled. *National Health Executive*. URL: https://www.nationalhealthexecutive.com/articles/wannacry-cyber-attack-cost-nhs-ps92m-after-19000-appointments-were-cancelled.

35. What Is Multi-Factor Authentication? *SoSafe*. URL: https://sosafe-awareness.com/glossary/multi-factor-authentication/.

36. LevelBlue - Open Threat Exchange. *LevelBlue Open Threat Exchange*. URL: https://otx.alienvault.com/.

37. CTI4SOC: Ultimate Solution to SOC Analyst's Biggest Challenges. *SOCRadar® Cyber Intelligence Inc.* URL: https://socradar.io/cti4soc-ultimate-solution-to-soc-analysts-biggest-challenges/.

38. How SOCRadar Can Help You with Threat Hunting? *SOCRadar® Cyber Intelligence Inc.* URL: https://socradar.io/how-socradar-can-help-you-with-threat-hunting/.

39. Analyze E-mail Threats in Seconds. Zero Miss for E-mail Threats. *Docguard*. URL: https://www.docguard.io/.

40. GreyNoise is the source for understanding internet noise. *GreyNoise*. URL: https://www.greynoise.io/.

41. Search Engine for the Internet of Everything. *Shodan*. URL: https://www.shodan.io/.

42. Fully Automate Your Tier 1 SOC. Deep, AI-powered investigations and autonomous triage for every endpoint, phishing, and SIEM alert. *Intezer*. URL: https://intezer.com/.

43. Intezer Analyze. By Intezer. Automate end-to-end malware investigations with genetic malware analysis. *Maltego*. URL: https://www.maltego.com/transform-hub/intezer-analyze/.

44. MISP - Open Source Threat Intelligence Platform. *CIRCL*. URL: https://www.circl.lu/services/misp-malware-information-sharing-platform/.

45. MISP Open Source Threat Intelligence Platform. *MISP*. URL: https://www.misp-project.org/.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)