Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Факультет комп'ютерних наук

Спеціальність 125 «Кібербезпека»

Освітня програма «Безпека інформаційних та комунікаційних систем»

«Допущено до захисту»
Зав.кафедрою БІСТ
Сергій РАССОМАХІН

_____

« » 2022 р.

Пояснювальна записка

до кваліфікаційної роботи магістра

на тему: «Аналіз розвитку та дослідження можливостей XDR-технології (Extended Detection and Response), як інструменту комплексної протидії сучасним загрозам ІБ»

оцінка « »

Голова ЕК

Доценко С.І. _____

Керівник доцент Малахов С.В.

Рецензент головний метролог

Гостев О.Л.

Виконавець : студент групи КБ-6

Погоріла К.В

Харків – 2022

РЕФЕРАТ

Пояснювальна записка містить: 77 сторінок, 13 рисунків, 7 таблиць, 59 використаних джерел, 1 додаток.

Мета роботи: - узагальнення відомостей, щодо можливостей використання XDR-технології (Extended Detection and Response), як основи для побудови комплексних корпоративних систем інформаційної безпеки.

Об’єкт дослідження: - технології і засоби комплексної протидії актуальним загрозам інформаційної безпеки (ІБ).

Предмет дослідження: - особливості інтеграції та використання XDR платформ безпеки в сучасних інформаційних системах (ІС).

Основними методами досліджень є аналіз та порівняння.

В роботі досліджено питання вразливостей сучасних корпоративних мереж та особливостей впровадження XDR технології, як нової концепції безпеки корпоративних ресурсів. Запропоновано аналіз існуючих технологій безпеки і шляхів розгортання та інтеграції XDR-систем. Підкреслено, що одна з основних переваг XDR-рішень – підвищення ефективності роботи персоналу відділів ІБ. Визначено, що імплементація переваг XDR, здійснюється за рахунок масштабної автоматизації процесів виявлення та реагування на переважну більшість інцидентів ІБ. Досліджено структуру сучасних загроз ІБ у корпоративному сегменті ринку та визначено специфіку реалізації відомих XDR-платформ. Представлена загальна оцінка відомих XDR-рішень.

Констатується, що технології розширеного виявлення та реагування мають ряд суттєвих переваг перед технологією EDR, а саме:

- підвищена швидкість виявлення загроз та реагування на них;

- збір та зіставлення даних з більш широкого спектра джерел;

- забезпечення глибшого моніторингу загроз, що дозволяє суттєво мінімізувати можливі наслідки і масштаб атаки.

- об'єднання різнорідних завдань та параметрів функціонування всіх складових діючої системи безпеки, в межах єдиного стеку ІБ.

Результати роботи можуть бути використані в освітніх цілях та, як допоміжний (довідковий) матеріал для розширення рівня професійної обізнаності персоналу підрозділів з ІБ.

Ключові слова: XDR, ИНФОРМАЦІЙНА СИСТЕМА, ЗАГРОЗА, ІНФОРМАЦІЙНА БЕЗПЕКА, EDR, SIEM, ШТУЧНИЙ ІНТЕЛЕКТ, ПІБ.

ABSTRACT

The explanatory note to the master's project contains: 77 pages, 13 figures, 7 tables, 59 source references, 1 appendix.

The purpose of the work: - summarizing information about the possibilities of using XDR technology (Extended Detection and Response) as a basis for building complex corporate information security systems.

The object of research: - technologies and means of comprehensive counteraction to current threats to information security (IS).

Subject of research: - features of integration and use of XDR security platforms in modern information systems (IS).

The main research methods are analysis and comparison.

The work is devoted the issue of vulnerabilities of modern corporate networks and the features of the implementation of XDR technology as a new concept of security of corporate resources. The analysis of existing security technologies and ways of deploying and integrating XDR systems is offered. It is emphasized that one of the main advantages of XDR-solutions is the improvement of the efficiency of the staff of IS departments. It was determined that the implementation of the advantages of XDR is carried out due to the large-scale automation of the processes of detection and response to the vast majority of IS incidents. The structure of modern IT threats in the corporate segment of the market was studied and the specifics of the implementation of known XDR-platforms were determined. A general assessment of known XDR solutions is presented.

It is noted that advanced detection and response technologies have a number of significant advantages over EDR technology, namely:

- increased speed of detecting threats and responding to them;

- collection and comparison of data from a wider range of sources;

- provision of deeper monitoring of threats, which allows to significantly minimize the possible consequences and scale of the attack.

- unification of disparate tasks and functioning parameters of all components of the current security system, within a single IS stack.

The results of the work can be used for educational purposes and as auxiliary (reference) material for expanding the level of professional awareness of the staff of IS units.

Key words: XDR, INFORMATION SYSTEM, THREAT, INFORMATION SECURITY, EDR, SIEM, ARTIFICIAL INTELLIGENCE.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ СКОРОЧЕНЬ І ТЕРМІНІВ

АРМ	–	Автоматизовані робочі місця
ЗЗІ	–	Засоби захисту інформації
ІБ	–	Інформаційна безпека
ІС	–	Інформаційна система
КЗ	–	Канали зв’язку
ПЗ	–	Програмне забезпечення
ПІБ	–	Політика інформаційної безпеки
СЗІ	–	Система захисту інформації
ШІ	–	Штучний інтелект
AI	–	Artificial Intelligence
API	–	Application Programming Interface
DLP	–	Data Leak Prevention
EDR	–	Endpoint Detection and Response
EDTR	–	Endpoint Detection and Threat Response
IDS/IPS	–	Intrusion Detection System / Intrusion Prevention System
MITM	–	Man-In-The-Middle
MTTD	–	Mean Time to Detect
MTTR	–	Mean Time to Repair
NGAV	–	Next Generation Antivirus
NGFW	–	Next-Generation Firewall
NTA	–	Network Traffic Analysis
SE	–	Social Engineering
SIEM	–	Security Information and Event Management
SOAR	–	Security Orchestration, Automation and Response

SOC	–	Security Operations Center
SOHO	–	Small office/home office
UEBA	–	User and Entity Behavior
UI	–	User Interface
USB	–	Universal Serial Bus
VPN	–	Virtual Private Network
XDR	–	Extended Detection and Response

ВСТУП

На сьогодні всі сучасні організації, які в межах своєї діяльності здійснюють зберігання, обробку і поширення даних, постійно стикаються з загрозами різного типу, що виходять як ззовні, так і з середини корпоративного контуру безпеки. Крім того, перенесення значної частини бізнес-процесів в хмару, фактично розмиває поняття корпоративного периметра безпеки, вимагаючи активного використання принципово нових концепцій та підходів у забезпеченні питань корпоративної ІБ, наприклад систем XDR-класу (тобто, розширені виявлення та реагування). Варто підкреслити, що перелік загроз стрімко розширюється, тому для забезпечення потрібного рівня безпеки інформаційних ресурсів, вкрай важливо постійно аналізувати відомі інциденти, всебічно оцінювати існуючи передумови виникнення загроз безпеки та своєчасно модифікувати наявну корпоративну політику ІБ (ПІБ).

Аналіз відомостей, стосовно найбільш резонансних інцидентів ІБ, свідчить про те, що відповідні акції здійснюються, як за допомогою залучення можливостей окремих інформаційних технологій (соціальні мережі, електронна пошта, месенджери, текстові повідомлення, форуми, комп'ютерні ігри та ін.), так і шляхом втілення концепції багаторівневої – інтегрованої атаки (наприклад, використовувати прийоми соціального інжинірингу, як одного із найпростіших способів отримання конфіденційної інформації). На фоні різкого збільшення кількості використання зловмисних програм-вимагачів та спроб організації витоку чутливих корпоративних даних (інсайду), а також зростанням загальної кількості атак на корпоративні інформаційні ресурси, чітко спостерігається тренд на значну професійну втому персоналу відділів безпеки, які повинні оперативно реагувати на всі спрацювання корпоративних засобів ІБ, та своєчасно проводити аудит відповідних інцидентів. Через всі ці труднощі, перелік яких, на жаль, с часом тільки збільшується, спеціалісти у сфері ІБ вимушені постійно вдосконалювати наявні технології та засоби забезпечення ІБ.

Серед останніх вдалих рішень слід підкреслити розробку та впровадження EDR технології (Endpoint Detection and Response) та SIEM- систем (Security Information and Event Management). Ці рішення в значної мірі полегшили контроль інцидентів ІБ в наступних напрямах: - блокування мережевих атак; - виявлення підозрілої активності; - глибоке логування подій; - безперервний збір інформації з контрольованих мережевих пристроїв. Крім того, SIEM-системи, в значній мірі сприяли вирішенню труднощів, щодо формування звітів ІБ, проведення розслідування (аудиту) інцидентів, та видачі оперативних оцінок, стосовно поточного рівня захищеності наявних інформаційних ресурсів. Однак, станом на сьогоднішній день, навіть такий перелік можливостей не є достатнім та залишає велику частку не вирішених труднощів.

Одним із перспективних рішень, щодо компенсації виниклих труднощів та посилення можливостей наявних корпоративних систем ІБ, є впровадження можливостей XDR технології, яка зменшує час реакції персоналу на переважну більшість інцидентів ІБ (тобто, з типовими поведінковими сигнатурами атак), та забезпечує помітно більш глибокий моніторинг, збір і узагальнення даних з більш широкого спектру джерел (в т.ч. програмних сенсорів).

Проте, слід зауважити, що неможливо реалізувати технологію, яка б вирішувала усі проблеми ІБ. Останнім часом, при розробці систем протидії інформаційним загрозам на перший план стає проблема гарантованого вирішення вже існуючих загроз та аналіз загроз, які можуть з’явитися при впровадженні тих чи інших рішень. Тому розгляд питань, стосовно можливостей протистояння цим викликам сучасного інформаційного суспільства, є безумовно актуальним, та потребує проведення ретельного аналізу і відповідних досліджень.

1 АНАЛІЗ ОСОБЛИВОСТЕЙ ТА СТРУКТУРИ СУЧАСНИХ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОРПОРАТИВНОМУ СЕГМЕНТІ ІТ-РИНКУ

На сьогоднішній день всі сучасні організації, котрі в межах своєї діяльності забезпечують зберігання, обробку і поширення даних постійно стикаються з загрозами безпеки різного типу, що виходять як ззовні, так і з середини корпоративного контуру інформаційної безпеки (ІБ). Під терміном ІБ будемо розуміти [2] стан певної інформаційної системи (ІС), при якому вона найменш вразлива до нанесенню збитку зі сторони зловмисника. Для підтримки потрібного стану ІБ ІС, необхідно забезпечити виконання наступних основних принципів безпеки: - цілісність; - конфіденційність; - доступність; - достовірність. Таке визначення ІБ ґрунтується на концепції, згідно з якою будь-якому об’єкту захисту (людині, бізнесу або уряду) буде завдано збитків, якщо порушені основні принципи ІБ. Отже, мета забезпечення ІБ ІС полягає в тому, щоб мінімізувати можливість прояви важких наслідків (в т.ч. фінансових і репутаційних).

На сьогоднішній день відомо про існування [3] понад 100 різновидів загроз ІБ для ІС різного типу та призначення, причому цей перелік постійно розширюється. Для забезпечення корпоративних ресурсів на потрібному рівні безпеки, вкрай важливо постійно слідкувати за появою нових загроз, ретельно і всебічно аналізувати всі ризики, та на їх основі своєчасно модифікувати існуючу систему ІБ. Загрози ІБ проявляються не самостійно, а через певні фактори вразливостей, що представлені на Рис.1.1.

Зазвичай джерела різних загроз ІБ активуються зловмисниками з метою отримання незаконної вигоди внаслідок заподіяння шкоди інформаційним ресурсам компанії. Але можлива й випадкова реалізація загроз через недостатність запроваджених мір захисту та/або масової дії факторів вразливості [4]. Існуючи класи вразливостей представлено на Рис. 1.2.

Загрози ІБ реалізуються за рахунок утворення відповідного «каналу» реалізації між джерелом загрози та носієм, що створює відповідні умови

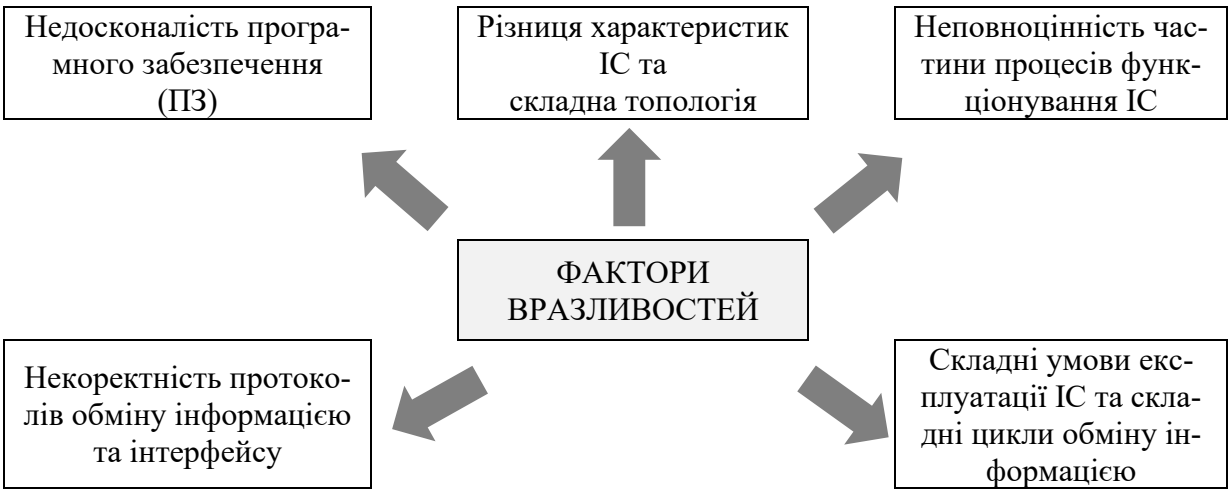


Рисунок 1.1 - Фактори вразливостей («слабкі» ланки системи захисту)

Класи вразливостей

ОБ'ЄКТИВНІ	**СУБ'ЄКТИВНІ**	**ВИПАДКОВІ**
Супутні засобам техн. випромінювання: • *електромагнітні* • *електричні* • *звукові* **Активізуючі:** • *апаратні закладки* • *програмні закладки* **Визначаються особливостями елементів:** • *елементи, що володіють електро-акустичними перетвореннями* • *елементи, що схильні до дії електромагнітного поля* **Визначаються особливостями об'єкта, що захищається:** • *розташуванням об'єкта* • *організацією каналів обміну інформацією*	**Помилки (халатність):** • *при підготовці та використанні ПЗ* • *при експлуатації технічних засобів* • *некомпетентні дії* • *ненавмисні та навмисні (інсайд) дії* • *дії під примусом* **Порушення** • *режиму охорони і захисту* • *режиму експлуатації технічних засобів і ПЗ* • *режиму використання інформації* **Психогенні** • *психологічні* • *психічні* • *фізіологічні*	**Збої і відмови** • *відмови та несправності технічних засобів* • *старіння і розмагнічування носіїв інформації* • *збої ПЗ* • *виробничі дефекти апаратних засобів* • *збої електро-постачання*

Рисунок 1.2 - Класи вразливостей

для порушення одного чи декількох ознак ІБ [3]. Головними елементами каналу реалізації загроз ІБ є [8]:

- джерело загроз, яке являє собою суб’єкт, здійснюючий загрози;

- середовище поширення інформації;

- носій, або матеріальний об’єкт, де інформація відображається у вигляді символів, технічних рішень і т.і.

Класифікація відомих загроз ІБ представлена в Табл.1.1.

Слід зазначити, що носіями загроз ІБ можуть бути як суб'єкти (особистість), так і об'єкти. Причому джерела загроз можуть перебувати, як в середині корпоративного периметру безпеки (внутрішні джерела), так і поза ним - зовнішні джерела. Як джерело загроз можна розглядати суб'єкта, що має доступ (санкціонований або несанкціонований) до роботи зі штатними засобами об'єкта, який захищається. Зовнішні джерела загроз ІБ можуть бути як випадковими, так і навмисними.[8]

До зовнішніх джерел загроз відносяться:

• кримінальні структури;

• потенційні зловмисники;

• недобросовісні партнери (в т.ч. представники IT-аутсорсінгу);

• конкуренти (конкуруючі організації);

• представники наглядових організацій і аварійних служб;

• представники силових структур;

• представники провайдерів послуг зв'язку та передачі даних;

• в деяких випадках - звичайні користувачі ІС.

Зовнішній порушник може здійснювати несанкціонований доступ:

• до каналів зв'язку (КЗ), які виходять за межі периметру безпеки;

• до автоматизованих робочих місць (АРМ), що мають підключення до мереж зв'язку і передачі даних, загального користування;

• через елементи існуючої інфраструктури ІС, які в процесі свого життєвого циклу (модернізації, ремонту, утилізації) тимчасово опиняються за межами контрольованих корпоративних зон безпеки;

Таблиця 1.1 - Загальна класифікація загроз

Критерій	Варіанти здійснення та сутність
За джерелом загроз	Антропогенні
	Технічні
	Стихійні
За способом реалізації	Витік інформації за допомогою технічних каналів
	Соціальна інженерія
	Спеціальний вплив на ІС
За принципом ІБ, що порушується	Загрози, що призводять до порушення конфіденційності інформації
	Загрози, що призводять до несанкціонованого впливу на зміст інформації
	Загрози, що призводять до можливості реалізації несанкціонованих дій персоналу ІС [52-53]
	Загрози, що призводять до несанкціонованого впливу на програмно-апаратні елементи ІС, в результаті якого здійснюється блокування інформації
За типом вразливості, що використовується	Вразливості системного ПЗ
	Вразливості прикладного ПЗ
	Вразливості апаратних засобів
	Вразливості протоколів мережевої взаємодії і каналів передачі даних
	Вразливості, що обумовлюють наявність технічних каналів витоку інформації
За об’єктом впливу	Реалізовані через автоматизовані робочі місця користувачів
	Реалізовані за допомогою впливу на сервери
	Зберігаються і оброблюються в засобах обробки
	Реалізовані в процесі взаємодії з КЗ
За видом активів (ресурсів), що схильні до загроз ІБ	Загрози безпеки даних, що зберігаються на робочих станціях користувачів
	Загрози безпеки даних, що зберігаються на серверах
	Загрози працездатності мережевих сервісів, обладнання та ПЗ робочих станцій і серверів, що викликані успішними атаками на відмову в обслуговуванні

• до корпоративної інформації з використанням спеціально створеного ПЗ та/або алгоритмічних або програмних закладок.

Також, зовнішні суб'єкти при певних умовах можуть перейти в групу внутрішніх (*наприклад, представники деяких наглядових служб можуть отримати можливість доступу до системи через її внутрішні інтерфейси*).

Внутрішніми суб'єктами (джерелами) загроз можуть виступати, як висококваліфіковані співробітники компанії (установи), так і співробітники з обмеженими компетенціями і повноваженнями доступу до корпоративних інформаційних ресурсів . До внутрішніх суб'єктів відносяться [8]:

• основний (функціональний) персонал;

• адміністративно-управлінський персонал;

• допоміжний персонал (бухгалтери, програмісти тощо);

• технічний персонал (слюсарі, прибиральники, охорона і т.п.).

Крім того особливу групу внутрішніх джерел загроз становлять особи з порушеною психікою, а також спеціально впроваджені ззовні (*наприклад, конкуруючою установою або державою*) співробітники [5]. Дана група розглядається в складі перерахованих вище джерел загроз, але методи парирування загроз, що обумовлені наявністю цієї групи, можуть мати свої відмінності [53].

З урахуванням обраного напряму досліджень, розглянемо більш детально питання стосовно внутрішніх загроз безпеки.

1.1 Інсадерські загрози

Інсайдерські загрози ІБ - це загрози, які виходять від штатних працівників організації. Важливо те, що саме ці загрози значно складніше піддаються вирішенню, ніж загрози технічного характеру. В зв'язку з цим слід зауважити, що ІБ - це не тільки питання технічних засобів контролю або заходів безпеки, а також і поєднання соціологічних та соціально-технічних методів [5]. Безпека інформації, яка обробляється в організації, – це комплекс дій, спрямованих на рішення проблеми захисту корпоративного інформаційного середовища. У будь-якому випадку кожний різновид корпоративної інформації мусить циркулювати та оброблятися, строго у визначену для нього сегменті мережі та передбачати допуск до неї тільки тих осіб, які регламентовані відповідними нормами і вимогами корпоративної політики ІБ (ПІБ) [6].

Особливу групу загроз в корпоративному сегменті безпеки посідає інсайд [6]. Інсайдерська інформація, або скорочено «інсайд» - це дані, які неправомірно отримані від співробітника будь-якої організації (установи, підприємства

і т.п.), та призначені тільки для «внутрішнього користування». Ця інформація, як правило не підлягає розголошенню, оскільки в разі витоку, може завдати чутливої шкоди для її власника. Як правило, інсайдерська інформація надходить, від інсайдерів - людей, що працюють в компанії, та в тій чи іншій мірі, мають допуск до чутливих корпоративних відомостей. Людина, що володіє інсайдом, особливо в разі існування якихось проблем в компанії, може представляти досить серйозну проблему (фінансову, репутаційну, юридичну і т.п.). [8]

Спираючись на щорічні дослідження відомих інцидентів витоку конфіденційної інформації (наприклад, від компанії InfoWatch*) [7], можна скласти відповідні рейтинги основних винуватців інсайду. Характерний приклад відповідних узагальнень за останні роки наведені на Рис. 1.3-1.5.

Рисунок 1.3— Дані InfoWatch за 2019 рік

На підставі ретельного аналізу та узагальнення щорічних досліджень відомих інцидентів витоку конфіденційної інформації можна зробити висновок, що на зовнішнього зловмисника відводиться більший відсоток інцидентів, ніж на штатно діючих співробітників. Але, при цьому, слід зауважити, що з кожним роком чисельність винуватців втрати важливих корпоративних відомостей внаслідок дій, саме співробітників компанії, зростає. Частка співробітників у 2019 р. знизилася до 41,4%, однак у наступні роки досягла 43%. Водночас у 2019-2021

роках. зростала частка витоків по вині керівників, але у 2021 р. вона трохи скоротилася.

У період пандемії збільшився обрій інциденту: у компаній більше часу займає виявлення витоку, опис шкоди та її усунення, в результаті відсувається час інформування про витік регуляторів та користувачів.

Рисунок 1.4 – Дані InfoWatch за 2020 рік

Рисунок 1.5 – Дані InfoWatch за 2021 рік

Як свідчить вивчення відомих випадків [7] , інсайдерські інциденти призводять до великих збитків*, як репутаційного, так й фінансового характеру.

Збитком інформаційного характеру слід вважати чутливі, для власника інформації, випадки, які пов'язані з втратою матеріального майна. Ці наслідки проявляються в результаті здійсненню певних правопорушення.

Заподіяти збиток ресурсам корпоративних ІС можна і шляхом зменшення прибутку або його недоотримання, що розцінюється, як втрачена вигода. Ступені та прояви збитків можуть бути такими:

- моральний і матеріальний збиток, нанесений фізичним особам, чия інформація була викрадена;

- фінансовий збиток, що є наслідком витрат на відновлення потрібного стану ІС або її системи ІБ;

- матеріальні витрати, які пов'язані з неможливістю продовження основних бізнес-процесів, через нештатні зміни в системі захисту інформації;

- моральний збиток, що пов'язаний з компрометацією репутації компанії.

У будь-якому випадку, в разі виявлення факту інсайда, вкрай важливо вчасно звернутися до суду та з'ясувати склад і обставини скоєння інциденту. Збиток потрібно класифікувати згідно з діючими правовими актами і довести його в судовому процесі. Крім того, важливо виявити ступінь особистої участі всіх фігурантів, що надасть змогу внести потрібні зміни до порядку забезпечення корпоративних норм. В залежності від масштабів понесених збитків і рівня значущості організації, що зазнала атаки, розслідуванням відповідних злочинів, може займатися кіберполіція або фахівці служба безпеки країни [3].

В цілому, в переважній більшості інцидентів, основною передумовою виникнення інсайдерських загроз є отримання вигоди за допомогою продажу корпоративної інформації конкурентам та/або ведення власного - тіньового бізнесу, за рахунок використання ресурсів компанії, зокрема й фінансових [6].

Існує багато різновидів інсайдерських загроз, однак спираючись на результати проведеного аналізу та узагальнення відомих інцидентів [7], в якості основних слід виділити наступні [8]:

- загроза витоку конфіденційної інформації в наслідок порушення порядку доступу до неї та/або її використання;

- нелегітимний доступ інсайдера до відомостей, стосовно порядку роботи технічних засобів наявної системи ІБ;

- ненавмисний витік конфіденційної інформації по необережності співробітників (тобто у інсайдера підтверджено відсутність будь-яких зловмисних намірів);

- неправомірне використання даних, що захищені авторським правом;

- нелегітимне отримання і навмисне використання фізичних засобів забезпечення та/або розмежування доступу до внутрішніх інформаційних ресурсів (наприклад, USB-токени, або чіп-картки працівників тощо) [7].

В даний час для протистояння інсайдерським загрозам та цілеспрямованим атакам організаціям необхідно приділяти особливу увагу не тільки рівню кінцевих точок, але й іншим потенційним точкам проникнення зловмисника в інфраструктуру та, найголовніше, взаємозв'язку між ними. Організації повинні мати розуміння того, що відбувається у них у рамках усієї інфраструктури, контролювати ключові точки проникнення та отримувати повну картину інциденту, мати можливість швидко аналізувати першопричини, проводити глибокі розслідування складних інцидентів та реагування на них у рамках усієї інфраструктури, а не окремих елементів.

З аналізу складових відомих порушень ІБ у 2021 р. продовжила зростати частка витоків з вини зовнішніх порушників, тобто хакерів, а також невідомих осіб з поза меж корпоративного контуру безпеки (їх дії по визначенню є навмисними). Ймовірно, суттєве зниження витоків внутрішнього походження багато в чому пов'язано з підвищеною латентністю відповідних інцидентів у період пандемії. У ході масового переходу персоналу на віддалену, а потім гібридну форму роботи, можна стверджувати що, у «тінь» стало йти суттєво більше порушень, у тому числі випадкового характеру (див. Рис.1.2 та Табл.1.1), які можна успішно детектувати за рахунок впровадження засобів безпеки на рівнях DLP (*Data Leak Prevention*) та XDR (*Extended Detection and Response*) рішень [34].

1.2 Огляд існуючих форм прояву соціального інжинірингу

З врахуванням останніх подій у світі і зростанням чисельності співробітників, що виконують свої посадові обов'язки в віддаленому режимі, кіберзлочинність активно зосереджується в удосконаленні технік нападу на окремих Інтернет користувачів, в тому числі, як проміжної цілі, для подальшого проникнення у внутрішній периметр безпеки компаній [12]. Еволюція соціальних мереж і той факт, що люди активно та абсолютно неуважно діляться великою кількістю персональної інформації про своє життя в Інтернеті, є головною причиною, що пояснює цю тенденцію.[8]

Як вже вказувалося раніше, загрози ІБ можуть мати технологічне (технічне) походження або обумовлюватися вразливостями антропогенного характеру, тобто вразливостями, що є наслідками присутності обслуговуючого персоналу. Використання прийомів соціального інжинірингу дозволяє конвертувати соціальні вразливості обслуговуючого персоналу компаній та установ в тимчасовий інструмент для здійснення (або сприяння для наступного здійснення) зовнішніх атак на інформаційні ресурси компаній. Соціальну інженерію можливо розглядати, як інструмент психологічного маніпулювання людьми з метою навмисного і системного створення умов для несвідомого виконання ними потрібних дій, та/або розголошення чутливої інформації (як корпоративної, так і особистої). Термін «соціальна інженерія» [13], як акт психологічної маніпуляції, перш за все, пов'язаний з соціальними науками, але в наслідок масштабної інформатизації сучасного суспільства, його використання помітно поширилося і серед фахівців з питань інформаційних технологій та ІБ.

Психологічна уразливість персоналу компаній, є важливою передумовою, що обумовлює створення широкого переліку різних каналів витоку чутливої корпоративної інформації. Така вразливість, перш за все, є наслідком поверхневого уявлення більшої частини співробітників про стан реальних загроз ІБ при використанні ними можливостей сучасних ІС та онлай сервісів. Атаки, що експлуатують фактор психологічної уразливості персоналу, зазвичай, використовують звички поведінки і довірливий характер користувачів ІС (наприклад, крадіжка

банківських кодів і даних автентифікації). SE-атаки (Social Engineering), зосереджені на маніпулюванні людьми (особистостями) і являють собою непомітну, однак, в певному сенсі, екзистенціальну загрозу для підтримки необхідних параметрів ІБ [13]. Для того, щоб протистояти впливу технологій соціальної інженерії, необхідно розуміння технік їх застосування. Розглянемо найбільш поширені форми і техніки соціальної інженерії.[8]

1.2.1 Огляд та узагальнення основних технік соціальної інженерії

Таксономія соціальної інженерії, що представлена на Рис. 1.6 (виділена сірим кольором) являє собою найбільш привабливі (поширені) методи сучасної кіберзлочинності.

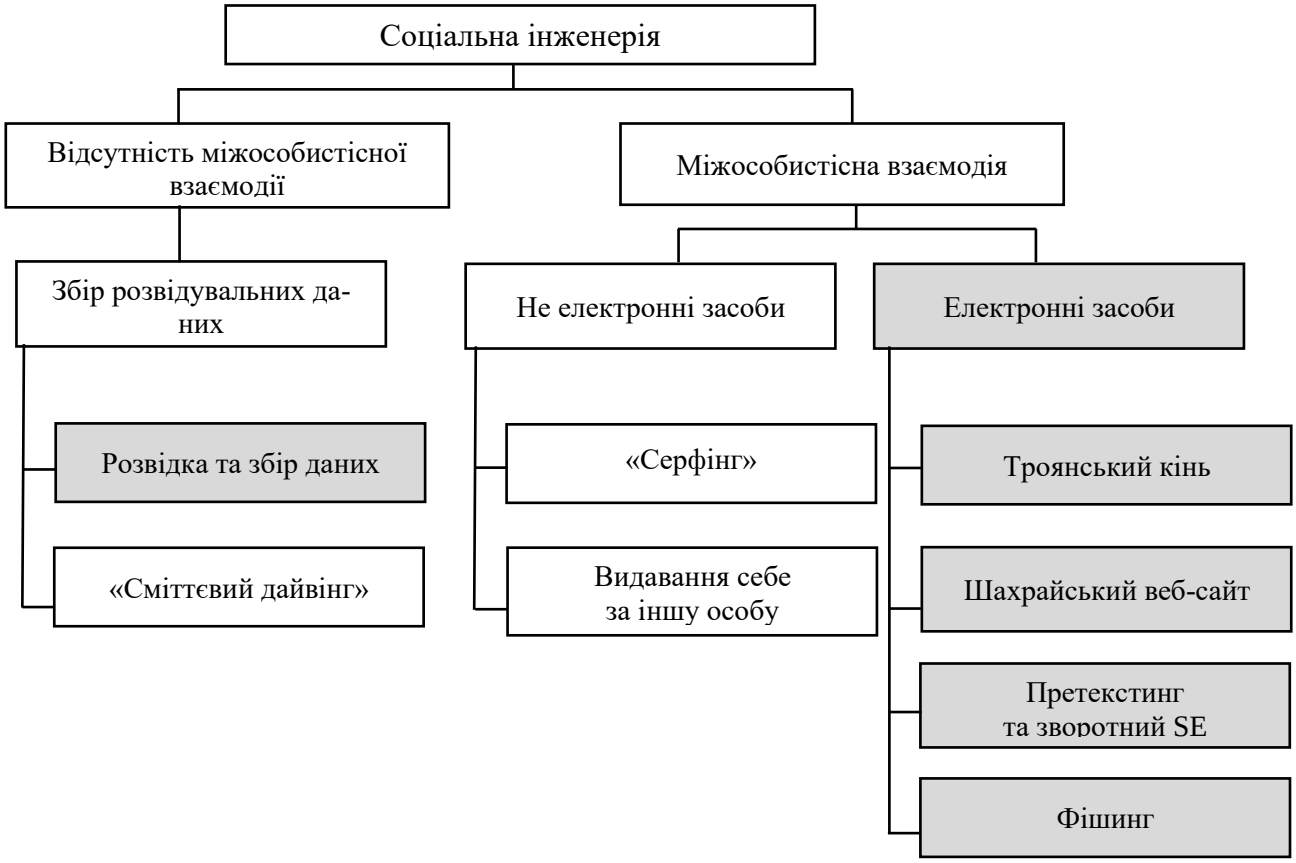


Рисунок 1.6 – Таксономія соціальної інженерії

Троянський кінь - ця техніка ґрунтується на різноманітних емоціях користувачів [1]. Зловмисник відправляє лист жертві за допомогою електронної пошти, в додатку до якого знаходиться, наприклад, оновлення якогось ПЗ, ключ до грошового виграшу або компромат на співробітника. Насправді ж у вкладенні

знаходиться шкідливе ПЗ, яке після його запуску буде використовуватися для незаконного збору або зміни інформації в системі користувача.[8]

Претекстінг - це система дій, відпрацьованих за певним, завчасно складеним сценарієм, в результаті якого жертва може ненавмисно розкрити будь-яку чутливу інформацію або вчинити певну дію. Здебільшого даний вид атаки передбачає використання зловмисником аудіовізуальних засобів, таких як Skype, телефон і т.п. Для використання цієї техніки зловмисникові необхідно обов'язково отримати якісь первинні дані про жертву (ім'я співробітника; посаду; назва проектів тощо) [14]. Т.ч. в ході атаки, зловмисник спочатку використовує реальні запити, спираючись на попередньо зібрану інформацію, і тільки після того, як увійде в довіру, отримує необхідну йому цільову інформацію.

Фішинг - техніка Інтернет-шахрайства, направлена на отримання конфіденційної інформації користувачів, як правило різних авторизаційних даних. Основною технікою здійснення фішингових атак є підроблений лист, відправлений жертві по електронній пошті, яке виглядає, як офіційний лист від будь якої установи або сервісу. В такому листі обов'язково міститься форма для введення персональних даних (*пін-кодів, логіна і пароля тощо*) або посилання на web-сторінку, де розташовується така форма. Причини довіри жертв подібним розсилкам можуть бути різні: блокування облікового запису, поломка в системі, втрата даних та інше.

Зворотний SE - це техніка нападу, що сфокусована на створенні такої ситуації, при якій жертва атаки буде змушена сама звернутися до зловмисника за «допомогою». Наприклад, зловмисник може завчасно вислати лист з контактами неіснуючої «служби підтримки», а через деякий час створити певні неполадки в устаткуванні та/або роботі ПЗ жертви. В такому випадку жертва атаки зв'яжеться з зловмисником сама, і вже в процесі «виправлення» проблеми зловмисник буде мати можливість для отримання потрібних йому відомостей [2].

Показовим прикладом цього типу атак, може служити інцидент, який трапився у 2017 році [13]. Громадянин Литви (Евальдас Рімаскаускас) був звинувачений в шахрайських діях по відношенню до двох міжнародних

телекомунікаційних компаній (одна з компаній спеціалізується на інтернет-сервісах і продуктах, а інша надає послуги онлайн-медіа та соціальних мереж). За два роки шахрайських дій (фішингової e-mail схеми), йому вдалося отримати від цих компаній більш ніж $ 100 млн. Цей випадок є дуже показовим, так як керівництво багато з сучасних IT- компаній до сіх пір вважають себе недоступними для вдалої реалізації SE атак.[8]

Отже, техніки і прийоми соціальної інженерії засновані на помилках і відхиленнях поведінки, мислення і сприйняття. Хитрість, гра на слабкостях і психології співробітників - все це і багато іншого використовується для отримання від людини необхідної для атакуючого інформації. Можна сформулювати базові методи SE, які використовуються шахраями та постійно вдосконалюються: 1 – фішинг (на сьогодні, э найпоширенішою схемою обману); 2- троянський кінь (експлуатуються жадібність і цікавість об'єкта атаки); 3 - перевтілення образу (тобто підміна особистості); 4 - претекстінг (прихована контекстна атака заздалегідь підготовленим сценарієм).

Довіра і впевненість, це фундаментальні поняття, що потрібні для підтримки безпечної взаємодії з будь-якою ІС. Звичка користувачів ділитися своєю інформацією, є прямим наслідком впливу фактора довіри, яку вони проявляють по відношенню до використовуваних ними соціальних мереж. Вплив довіри до соціальних мереж і, звичайно ж, способи її зловживання - це перспективний та багатогранний напрямок окремих досліджень.

Отже, для забезпечення базового рівню захисту від найбільш поширених методів SE-атак, треба знати найбільш поширені (актуальні) форми і техніки SE, а також шляхи протидії проявам цього небезпечного інструменту маніпулювання персоналом. Одним з таких шляхів є впровадження XDR рішень, що забезпечує покращення можливостей виявлення, реагування та оптимізації продуктивності корпоративного SOC (Security Operations Center), надаючи цілісне уявлення про поточні загрози ІБ в усьому стеку технологій безпеки організації. XDR технологія надає інформацію та дані для виявлення та реагування на сучасні загрози

шляхом інтеграції засобів контролю безпеки, таких як кінцева точка та мережа, дані та аналітика та SecOps.

Впровадження XDR в певної мірі компенсує критичну нестачу персоналу з питані забезпечення ІБ. Галузеві експерти сходяться на думці, що варто спостерігати все більшу інтенсифікацію впровадження цих рішень, як способу боротьби з одночасним збільшенням частоти та складності кібератак [15]:

-70% фахівців із безпеки вважають, що їх організація вже офіційно інвестує в XDR, або планує зробити це протягом наступних 6 місяців;

- понад 80% організацій планують збільшити інвестиції в технології виявлення загроз і реагування на них.

2 ОГЛЯД СУЧАСНИХ КОНЦЕПЦІЙ ТА ТЕХНОЛОГІЙ ЗАХИСТУ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Безпека корпоративних даних - одне з головних завдань, які вирішуються IT-відділами компаній. Причому йдеться не лише про запобігання витоку корпоративної інформації, зниження обсягів зловмисного трафіку та відображення атак на ресурси компанії, а й про оптимізацію роботи системи безпеки в цілому. Знайти універсальне рішення у цьому питанні складно.

Забезпечення ІБ є актуальним для будь-якої організації, оскільки сьогодні всі бізнес-процеси активно переходять у віртуальний простір: оплата товарів та послуг через Інтернет, електронна пошта, IP-телефонія, хмарні сховища, віртуальні сервери тощо. Нажаль корпоративні мережі більшості організацій побудовані з використанням обладнання різних поколінь і від різних виробників, що помітно ускладнює процес управління IT- системою, що робить корпоративні ресурси особливо вразливими. В цьому контексті, головними завданнями при створенні та експлуатації будь-якої сучасної системи ІБ є:

-забезпечення доступності даних для авторизованих користувачів, та можливості оперативного отримання основних інформаційних послуг;

- гарантії цілісності інформації, її актуальності та захищеності від несанкціонованої модифікації та/або знищення;

- недопущення реалізації несанкціонованих дій персоналу [52,53], особливо при реалізації критичних операцій та/або циклів управління в межах діючих корпоративних ІС (наприклад, централізоване відключення функцій логування систем ІБ та/або знищення корпоративних баз даних тощо);

- забезпечення конфіденційності відомостей, що циркулюють в межах забезпечуваного жах контуру безпеки.

Для вирішення зазначених вище завдань застосовуються такі методи захисту інформації, як: - протоколювання, ідентифікація і аутентифікація, управління доступом, використання сумісних дій персоналу при виконання найбільш

відповідальних (критичних) процедур управління [53], використання міжмережевих екранів та технології Honey Pot [22] та криптографічний захист.

Надійний захист інформаційних ресурсів забезпечує лише комплексний підхід, що передбачає одночасне використання апаратних, програмних та криптографічних засобів (жоден із цих засобів окремо не є достатньо надійним). Подібний підхід як раз передбачає впровадження XDR платформ, що забезпечує аналіз і оптимізацію всієї наявної системи безпеки, а не окремих її частин, що дозволяє забезпечити баланс характеристик ІБ, тоді як покращення одних параметрів нерідко призводить до погіршення інших.

Організаційні заходи, які вживаються при комплексному підході, є самостійним інструментом і об'єднують усі методи, що використовуються в межах корпоративній ПІБ, в єдиний цілісний захисний механізм. Це забезпечує безпеку даних на всіх етапах їх життєвого циклу [46].

До основних програмно-апаратних засобів безпеки відносяться:

1) Міжмережеві екрани. Вони забезпечують поділ мереж та запобігають порушенню користувачами встановлених правил безпеки. Сучасні міжмережові екрани відрізняються зручним керуванням та великим функціоналом (можливістю організації VPN (Virtual Private Network), інтеграції з антивірусами та ін.). В даний час спостерігаються тенденції:

- до реалізації міжмережевих екранів апаратними, а не програмними засобами (це дозволяє знизити витрати на додаткове обладнання та ПЗ та підвищити ступінь захищеності);

- до впровадження персональних міжмережевих екранів;

- до орієнтації на сегмент SOHO (Small office/home office), що призводить до розширення функціоналу цих засобів.

2) Антивірусний захист інформації. Антивірусні системи захищають робочі станції, а також закривають поштові шлюзи, проксі-сервери та інші шляхи проникнення вірусів. Ефективним рішенням є паралельне використання двох і більше антивірусів, у яких реалізовано різні методи виявлення шкідливого ПЗ.

3) Системи виявлення та запобігання атак (IDS/IPS- Intrusion Detection System / Intrusion Prevention System). Подібні системи тісно інтегровані із засобами блокування шкідливих впливів та з системами аналізу захищеності. Система кореляції подій акцентує увагу адміністратора лише на тих подіях, які можуть завдати реальної шкоди інфраструктурі компанії. [32]

4) Контроль доступу та засоби захисту інформації всередині мережі. З метою забезпечення безпеки даних великими компаніями проводиться автоматизація управління інформаційною безпекою або створення спільної консолі управління, а також розмежування доступу між співробітниками відповідно до їхнього функціоналу. В області засобів створення VPN відзначається прагнення до підвищення продуктивності процесів шифрування та забезпечення мобільності клієнтів (тобто доступу до інформації з будь-якого пристрою). Розробники систем контролю вмісту прагнуть домогтися того, щоб створені ними системи не створювали дискомфорту користувачам [48].

Комплексні програмні рішення допомагають захистити весь інформаційний периметр та запобігти більшості ситуацій, пов'язаних з діями інсайдерів або атаками хакерів. Слід виділити такі типи програмних засобів, що застосовуються в галузі інформаційної безпеки:

- засоби контентного аналізу;
- засоби криптографічного захисту;
- DLP- системи.

Серед окремих пропозицій ринку необхідно виділити рішення контентного аналізу (в т.ч. на рівні корпоративних proxi) та протидії ведення мережевої розвідки [22]. Вони допомагають фільтрувати трафік, що спрямовується на зовнішні маршрутизатори та сервери в DMZ-зонах [34] в межах загальнодоступних (публічних) сегментів корпоративної IT- інфраструктури. Зазвичай ці засоби захисту встановлюються в «розрив» між корпоративною мережею і виходом в іншу, «зовнішню» мережу. Обробка даних відбувається шляхом їх «розбиття» на службові поля, всередині яких йде фільтрація за критеріями, що задані службою безпеки та/або настроюваннями відповідних програмно-апаратних засобів. Але

більшість цих механізмів не працюють, або працюють з великою дискретністю («так», чи «ні»), якщо повідомлення (трафік) перед відправкою було зашифровано та/або були застосовані стеганографічні методи обробки контенту (безвідносно типу носія-контейнеру даних) [55,56].

Криптографічні засоби допомагають зашифрувати дані, що знаходяться на жорстких дисках, на знімних носіях, пакетах даних, що передаються каналами зв'язку. Ключі, зазвичай, зберігаються на окремому носії, який знаходиться в захищеному місці. Навіть розкрадання жорсткого диска в цьому випадку унеможливить розшифровку конфіденційної інформації.

Крім встановлення ПЗ та створення оптимальної конфігурації для діючої системи ІБ, в рамках реалізованих організаційних та технічних заходів потрібно систематично проводити перевірки для виявлення заставних пристроїв – електронних пристроїв перехоплення інформації – та для проведення спеціальних досліджень на побічні електромагнітні випромінювання та наведення. Для організації таких перевірок використовують спеціальну апаратуру [48]. Забезпечуючи охорону певної зони, приділяють увагу пропускному режиму на контрольованій території та забезпечують виявлення прихованих засобів електромагнітних випромінювань, що виходять від усіх візитерів – від клієнтів та контрагентів до ремонтних служб, адже кожен з них може пронести в периметр, закладний пристрій – перехоплювач звукової інформації.

Т.ч. тільки одночасна комбінація всіх компонентів технічної та організаційної складових заходів ІБ, дозволяє досягти успіху з протидії сучасним загрозам. Тому поява технології, яка поєднує в собі основні вектори захисту від атак на всіх відомих рівнях їх реалізації, є вкрай важливою подією. Технологія XDR [42] пропонує нову модель захисту, яка включає одночасний контроль подій на багатьох «ділянках» за допомогою мережевих сенсорів, а також міжмережевих екранів, шлюзів безпеки, IDS/IPS, NTA (Network Traffic Analysis), поштових і DLP- систем, IDM/IAM, SIEM(Security Information and Event Management). Вся ця інформація аналізується в єдиному комплексі, і до того ж можна налаштувати реагування на можливу атаку на будь-якому рівні. Також XDR дозволяє

проводити більш глибоке розслідування інцидентів, починаючи з «нульової дії», коли він спробував проникнути в інфраструктуру. Це дозволяє практично повністю контролювати всі можливі канали реалізації загроз в інфраструктурі підприємства.

Відомі рішення XDR поєднують у собі кілька інструментів, формуючи єдину платформу виявлення інцидентів у безпеці та реагування на них. Так, XDR дозволяє комплексно контролювати можливі вектори атак на IT інфраструктуру та її інформаційні ресурси, шляхом збору поточних даних на наступних рівнях мережевої інфраструктури:

- кінцеві точки;
- мережевий рівень (шлюзи безпеки, FW, IPS, WAF, мережеві сенсори),
- хмарні середовища та хмарні сервіси [34];
- контроль запуску (ініціювання роботи) корпоративних гіпервізорів [52];
- поштовий трафік,
- системи управління доступом,
- засоби верифікації користувачів [57];
- DLP-системи та ін.

Таким чином, за рахунок розгортання XDR можна побачити всі етапи атаки і дізнатися, якою була перша дія, з якої почалося проникнення в мережу підприємства. Процеси збору та аналізу подій побудовані на автоматичних діях системи та машинному навчанні, що дозволяє скоротити кількість адміністраторів безпеки, які відповідають за реагування та розслідування інцидентів.

Отже, сьогодні існує велика кількість технологій різних класів для моніторингу кіберзагроз і захисту від них. З одного боку, це дозволяє закрити основні вектори атак. З іншого боку, службам ІБ доводиться одночасно працювати з величезною кількістю різнорідних рішень безпеки і аналізувати безліч розрізнених даних. Як наслідок, вони регулярно втрачають найцінніший ресурс - час, відведений на реагування, а ризик компрометації важливих даних та/або процесів при цьому зростає. Рішення класу XDR покликані вирішити такі складності.

3 ЕВОЛЮЦІЯ РОЗВИТКУ ТА СТРУКТУРА ОСНОВНИХ СКЛАДОВИХ XDR-ТЕХНОЛОГІЇ

З кожним роком підходи кіберзлочинців стають все більш продуманими та швидко адаптованими до нових реалій, тому організації поступово нарощують потенціал наявних засобів забезпечення ІБ і все це, нажаль, представляє собою велику кількість не інтегрованих між собою ІБ інструментів, у тому числі щодо виявлення та реагування на ІБ - інциденти, та низки відповідних консолей управління безпекою.

Профільним фахівцям добре відомі інструменти кіберзахисту, які схожі з XDR, але через свою більш вузьку спеціалізацію, в них помітно менше спеціалізованих функцій. Так, наприклад:

- EDR (Endpoint Detection and Response) забезпечують захист лише на рівні кінцевих точок, без мережевих та хмарних служб;
- SIEM-системи здійснюють лише збір і аналіз інформації у внутрішній мережі, без функцій реагування на випадки;
- UEBA (User and Entity Behavior) аналізують лише поведінку користувачів, пристроїв і програм, без реагування на їх аномалії;
- SOAR(Security Orchestration, Automation and Response) охоплюють більшу частину корпоративної IT інфраструктури, але працюють, в основному, за сигнатурами та типовими сценаріями реагування, не забезпечуючи проактивний захист ресурсів. При цьому, в SOAR помітно нижчий рівень сумісності з іншими рішеннями та додатками, що є джерелами даних;
- NTA-системи обмежені аналізу мережевого трафіку та виявлення складних (цільових) атак.

3.1 Виявлення та реагування на кінцеві точки (EDR)

Виявлення та реагування на кінцевих точках (EDR), також відоме як виявлення кінцевих точок і реагування на загрози (EDTR-Endpoint Detection and

Threat Response), — це рішення безпеки кінцевих точок, яке постійно відстежує стан безпеки на рівні пристрої кінцевих користувачів корпоративної мережі, що має 2 вектори зусиль: - може виявляти та реагувати на ІБ. Рішення безпеки EDR фіксують (тобто складають детальні лог-файли) мережеву активність, що відбуваються на кінцевих точках, надаючи групам безпеки можливості поточного аналізу подій, необхідні для виявлення інцидентів, які в іншому випадку залишаються невидимими. Рішення EDR забезпечує постійну та повну видимість того, що відбувається на кінцевих точках у режимі реального часу.

Проведений огляд дозволяє констатувати, що інструменти EDR пропонують розширені можливості стосовно виявлення загроз, розслідування та реагування, включаючи пошук даних про інциденти і сортування сповіщень про розслідування, перевірку підозрілих дій, відстежування на загрози, а також виявлення, та запобігання шкідливих дій (див. Рис 3.1).

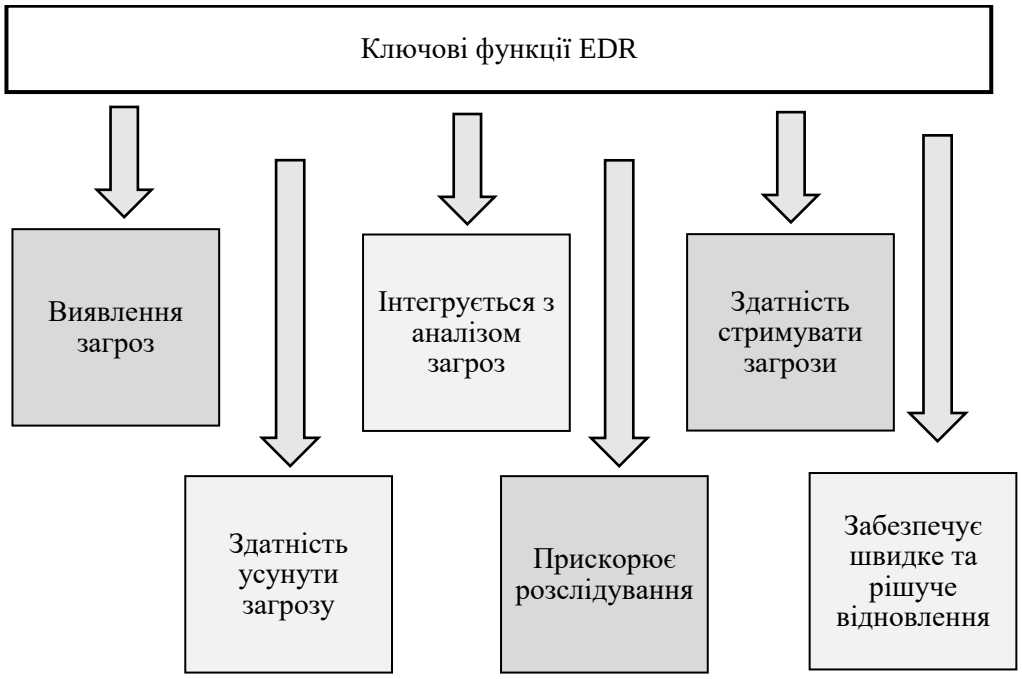


Рисунок 3.1- Ключові функції EDR

Виявлення загроз є основною можливістю EDR. Завдяки безперервному аналізу загроз, EDR може позначати шкідливі файли за перших ознак зловмисної (підозрілої) поведінки. Якщо файл вважається безпечним, але, наприклад, через

кілька тижнів починає проявляти активність криптомайнінгу, EDR виявить цей файл і ініціює процес аналізу його поведінки і оцінки можливих ризиків, попередивши відповідний персонал про необхідність вжиття відповідних заходів.

Після виявлення шкідливого файлу (або не декларованої активності) EDR здатний стримувати цю загрозу. Зазвичай шкідливі файли спрямовані на компрометацію якомога більшої кількості процесів, програм і користувачів, тому сегментація наявних мережевих ресурсів, може стати ефективним захистом у центрі обробки даних, щоб уникнути горизонтального переміщення актуальних (або ще невідомих) загроз. Як додатковий контроль EDR надає можливість ізолювати мережу, яка скомпрометована, запобігаючи таким чином, подальшому розповсюдженню в мережі, нових типів атак (загроз).

Після того, як шкідливий файл (процес) виявлено та локалізовано, EDR проводить аудит випадку. EDR визначає тип аналізу кожного інциденту, який необхідний для виявлення цих проблем та запобігання майбутньому використанню через той же самий вектор загрози, коли це можливо.

Отже, традиційні інструменти EDR зосереджені лише на даних кінцевих точок, забезпечуючи обмежену видимість потенційних загроз ІБ. Це може призвести до пропусків виявлення, збільшення хибних спрацьовувань і довшого часу аудиту інцидентів. Ці недоліки ускладнюють труднощі, з якими вже стикаються багато фахівців з ІБ, включаючи перевантаження подіями, брак навичок, вузькоспеціалізовані інструменти, брак інтеграції та дефіцит часу.

3.2 SIEM-системи

SIEM-системи забезпечують аналіз подій в реальному часі, що відбуваються в корпоративній IT -інфраструктурі. Такий аналіз необхідний для виявлення і визначення серед усіх подій саме тих, що погрожують поточному стану ІБ. SIEM-система збирає, аналізує та представляє інформацію з мережевих пристроїв і пристроїв безпеки. Крім того, в цю систему входять додатки для управління ідентифікацією і доступом, та інструменти управління важливими базами даних, і додатків.

Наявність в складі корпоративного контуру безпеки працюючої SIEM системи є одним із ключових показників того, що організація має чітко визначену політику ІБ (ПІБ). Робота SIEM системи (див. Табл. 3.1) забезпечує більш повну картину активності мережі та подій безпеки.

Таблиця 3.1 – Функціональні можливості SIEM-систем

Функціонал	***Особливості реалізації***
Агрегація даних	Збирає та створює журнали з кількох IT-систем та об'єднують їх у стандартизований набір даних, що зберігається централізовано, до якого можуть запитувати групи безпеки та використовувати для створення автоматичних сповіщень.
Кореляція подій та аналітика	Аналізує дані журналу та використовує правила кореляції та статистичний аналіз для виявлення можливих інцидентів безпеки. Наприклад, SIEM може ідентифікувати невдалу спробу входу одного користувача на кількох кінцевих точках, серверах і хмарних службах.
Сповіщення безпеки	Надсилає сповіщення групам безпеки через інтерфейс SIEM або через різні канали сповіщень. Сповіщення надають детальну інформацію про подію та дозволяють аналітикам сортувати та досліджувати інцидент далі.
Дослідження даних	Зберігає дані про події, що дозволяє аналітикам ІБ шукати та досліджувати дані протягом певного періоду часу, використовуючи запити SQL, у рамках розслідування інцидентів або проактивного пошуку загроз.
Управління відповідністю	Використовує програми автоматизації збору даних відповідності, створюючи звіти, які адаптовані до існуючих процесів безпеки, управління та аудиту.
Зберігання	Забезпечує довгострокове зберігання накопичених даних для полегшення аналізу і кореляції даних у часі та забезпечення збереження, необхідного для відповідності вимогам «довгого» аудиторського сліду.

Узагальнюючи відомості Табл. 3.1, можна стверджувати, що SIEM системи необхідні компаніям для роботи з великим потоком різнорідних даних від різних джерел з метою виявлення потенційних інцидентів ІБ та своєчасного реагування на них. SIEM - це інструмент збору журналів, призначений для підтримки відповідності, зберігання і аналізу даних. Аналітика ІБ – це функція, яка в основному, включена в рішення SIEM і не дозволяє належним чином ідентифікувати загрози без запуску окремої функції аналітики безпеки «поверх» величезного обсягу різнорідних даних.

3.3 Аналітика поведінки користувачів і об’єктів (UEBA)

Аналітика поведінки користувачів і об’єктів (UEBA) - це рішення безпеки, яке використовує алгоритми та технології машинного навчання для виявлення аномалій у поведінці не лише користувачів корпоративній мережі, але й маршрутизаторів, серверів і кінцевих точок у цій мережі (тобто, наявного мережевого устаткування).

UEBA використовує машинне навчання, алгоритми та статистичний аналіз для фіксації поточних відхилень мережевої активності від встановлених шаблонів, показуючи, яка з цих аномалій може призвести до реальної загрози. UEBA також, поєднує дані, які містяться у звітах і журналах, а також аналізує інформацію про файли, потоки та пакети, що циркулюють в мережі.

Основне завдання UEBA (див. Табл. 3.2) – своєчасно виявляти цільові (заздалегідь сплановані) зовнішні атаки та парирувати інсайдерські загрози. Відповідно завданням, рішення UEBA оброблюють великий обсяг даних з різних джерел, визначають штатні моделі поведінки для кожного користувача контрольованої мережі та/або об'єкта та повідомляють ІБ-фахівців, якщо помічають відхилення від цих моделей.

UEBA тісно пов’язана з SIEM, оскільки виконує багато подібних функцій - вона також збирає цільові відомості з корпоративної мережі, аналізує їх і генерує сповіщення. Однак, у той час як рішення UEBA в більшої мірі зосереджені на аналізі, то системи SIEM охоплюють дуже великі обсяги даних безпеки,

організовують їх для аналітиків безпеки та забезпечують структуровані процеси в SOC.

Таблиця 3.2- Основні завдання UEBA

Функціонал	***Особливості реалізації***
Виявлення внутрішніх загроз	UEBA виявляє витоки даних, саботаж, зловживання привілеями та порушення політики вашими власними співробітниками.
Виявлення зламаних облікових записів	Блокує підроблених і скомпрометованих користувачів, перш ніж вони зможуть завдати реальної шкоди.
Виявлення атаки грубої сили	Виявляє спроби «грубої сили» (наприклад, брудфорс, DDos тощо), дозволяючи блокувати доступ до цільових об’єктів.
Виявлення змін в дозволах і створення суперкористувачів	Визначає випадки, коли створено «суперкористувачів» або чи є облікові записи, яким надано занадто непотрібні дозволи (повноваження).
Виявлення порушень захищених даних	Виявляє, коли користувач отримує доступ до захищених даних, якщо він не має жодних прав доступу до них (контроль рівнів доступу до БД).

3.4 Управління безпеки, автоматизація та реагування (SOAR)

SOAR) відноситься до набору програмних рішень та інструментів, які дозволяють організаціям оптимізувати операції безпеки в трьох ключових сферах: - управління загрозами та вразливостями, реагування на інциденти і автоматизація операцій безпеки. Управління загрозами та контроль вразливостей поєднує технології, які допомагають безпосередньо протидіяти загрозам, тоді як автоматизація операцій безпеки (автоматизація) пов’язана з технологіями, що забезпечують автоматизацію та адміністрування профільних операцій ІБ.

Управління загрозами (або адміністрування) це здатність системи координувати прийняття рішень і автоматизувати відповідні дії, на основі оцінки ризиків та стану контрольованого мережевого середовища. Інструменти SOAR роблять це шляхом інтеграції з іншими рішеннями безпеки. SOAR надає загальний інтерфейс, що дозволяє визначати потрібні дії, стосовно інструментів безпеки та IT-систем, для персоналу, що не є експертами в цих системах або їх API (Application Programming Interface).

Автоматизація пов’язана з адмініструванням, практично це, кероване виконання дій з наявними програмно-апаратними засобами безпеки та IT-системами (телекомунікаційним устаткуванням), в рамках оперативного реагування на інцидент ІБ. - Інструменти SOAR (див. Рис. 3.2.) визначають стандартизовані етапи автоматизації та робочий процес прийняття рішень, із можливостями примусового виконання, відстеження стану та аудиту.

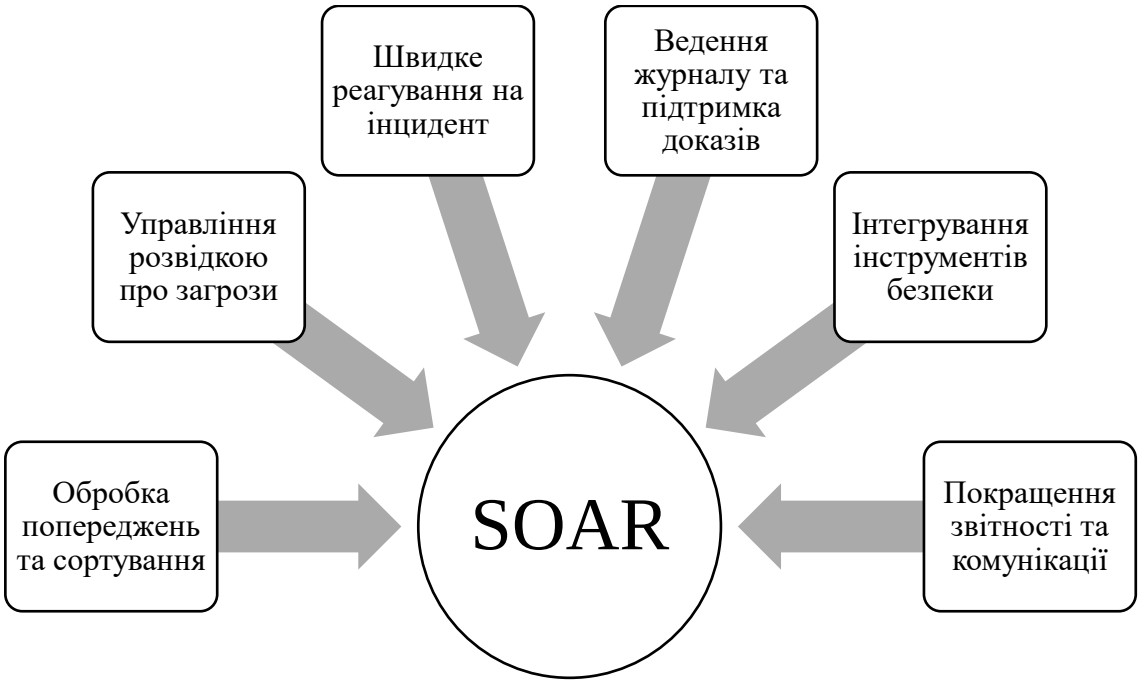


Рисунок 3.2 – Основні можливості SOAR

Управління інцидентами ІБ та тісна взаємодія - допомагають персоналу з ІБ, керувати інцидентами безпеки та обмінюватися даними з іншими групами фахівців, що вирішують аналогічні питання з протидії подібним інцидентам.

Слід зазначити, що платформа SOAR дозволяє системно адмініструвати і автоматизувати процес сповіщення та реагувань на інциденти. Відфільтровуючи повсякденні завдання, які забирають найбільше часу, зусиль та ресурсів, робочі групи з ІБ, забезпечують більш ефективну обробка та розслідування інцидентів, що значно покращує загальну безпеку організації. Т.ч. інструменти SOAR надають можливості (див. Рис. 3.2.), які допомагають центрам безпеки (SOC) ефективніше та оперативніше реагувати на інциденти з ІБ.

SOAR, як зазначалося вище, включає управління, автоматизацію та можливості реагування на інциденти, що дозволяє розрізненим інструментам безпеки координувати один з одним, в рамках єдиного сценарію протидії актуальним загрозам. Незважаючи на цінність, SOAR не вирішує проблему аналітики великих даних та не захищає дані чи системи самостійно [27].

3.5 Аналіз мережевого трафіку (NTA)

Аналіз мережевого трафіку (NTA) - це метод моніторингу доступності та активності мережі для виявлення аномалій трафіку і поведінки користувачів, зокрема проблем із безпекою та функціонуванням. Загальні випадки використання NTA включають:

- збір даних про те, що відбувається у мережі в режимі реального часу та за попередні періоди;
- виявлення активності зловмисного програмного забезпечення;
- виявлення випадків використання вразливостей протоколів і шифрів (експлуатація експлойтів) [51,54,8];
- покращення параметрів поточного моніторингу та усунення «сліпих» зон мережі;

Слід підкреслити три ключові відмінності NTA-систем від інших рішень, що працюють з мережевим трафіком:

1) NTA-системи аналізують трафік і на периметрі, і безпосередньо в інфраструктурі. Наприклад, інші рішення, що працюють із трафіком (IDS/IPS, міжмережеві екрани), стоять, як правило, на зовнішньому периметрі

безпеки. Тому, коли зловмисники проникають в мережу, їх дії вже залишаються непоміченими.

2) NTA-системи виявляють атаки за допомогою комбінації таких інструментів, як: - машинне навчання, поведінковий аналіз, правила детектування, індикатори компрометації, глибокий (прецедентний) аналіз подій. Така комбінація дозволяє виявляти атаки на ранніх стадіях та/або коли зловмисник уже проник в інфраструктуру.
3) Застосування NTA допомагає у розслідуванні інцидентів та проактивному [29] пошуку загроз, які виявляються традиційними засобами безпеки. NTA-системи зберігають інформацію про мережеві взаємодії, що є корисними джерелами при локалізації атак.

Аналіз мережевого трафіку є дуже важливим способом моніторингу доступності і активності мережі для виявлення потенційних аномалій, покращення продуктивності мережевого телекомунікаційного обладнання та спостереження за атаками. Поряд із агрегацією журналів, даними UEBA та кінцевими точками, поточні параметри мережевого трафіку є основною частиною для всебічного аналізу стану безпеки для раннього виявлення загроз і їх швидкого попередження. Проте, рівень компетенції інструментів аналізу мережевого трафіку (NTA) об'єктивно обмежений рамками контрольованої мережи та/або її окремими сегментами, з усіма наслідками.[33]

Таким чином, можна зробити висновок, що всі ці рішення спрямовані на протистояння кіберзагрозам, але одні з них «закривають» лише окремі вектори можливих атак (локальна мережа, Е-пошта, хмара та ін.), інші ж, навпаки, відповідають за певні дії в рамках процедур реагування на інциденти (наприклад, виявлення, реагування, запобігання подій тощо). Експлуатація таких рішень має різний рівень кінцевого успіху, але найчастіше профільні відділи компаній і установ, страждають від надзвичайно високого споживання наявних ресурсів та переважання несистематичним підходом до змісту та послідовності обробки інцидентів.

4 ОГЛЯД МОЖЛИВОСТЕЙ ТА ДОСЛІДЖЕННЯ СПЕЦИФІКИ РЕАЛІЗАЦІЇ XDR-ТЕХНОЛОГІЇ, ЯК ЗАСОБУ КОМПЛЕКСНОЇ ПРОТИДІЇ АКТУАЛЬНИМ ЗАГРОЗАМ ІБ

На сьогоднішній день далеко не всі організації можуть дозволити собі мати штат фахівців з питань інформаційної безпеки (ІБ) для ефективної експлуатації всіх наявних у них систем та/або інструментів забезпечення ІБ, у рамках єдиного процесу роботи з інцидентами безпеки, оскільки глобальна нестача кваліфікованих профільних кадрів, продовжує залишатися ключовою проблемою на ринку праці. Більш того, велика кількість консолей управління та труднощі з інтеграцією між різними рішеннями ІБ, є причиною неможливості зіставлення подій, що отримані із різних джерел у єдиний інцидент, а також нестачі прозорості в масштабах усього підприємства. Все це веде до формування т.з. «сліпих зон» в контурі безпеки ІБ і супроводжується великою кількістю «ручних» завдань, що погіршує показники середнього часу виявлення та реагування на загрози (MTTD - Mean Time to Detect та MTTR - Mean Time to Repair).

Зазначений набір труднощів потребує пошуку якогось рішення. Замість того, щоб розширювати наявний корпоративний арсенал розрізненими інструментами і засобами забезпечення ІБ, організації концентрують увагу на питаннях уніфікації їх захисту та підвищення ефективності роботи персоналу, котрий залучається для забезпечення питані ІБ. Саме для вирішення подібних труднощів було розроблено клас XDR рішень , що входить до трійки найкращих проектів у галузі кібербезпеки у 2021 році [11].

XDR виник як розвитку засобів виявлення та реагування на кінцеві точки (EDR), визнаючи потребу у «видимості» загроз, яка була би глибшою, ніж в SIEM, але при цьому, не обмежувалася кінцевими точками. Таким чином, XDR прискорює розслідування інцидентів та використовує автоматизацію для збільшення продуктивності членів груп безпеки (в т.ч. прискорення пошуку необхідних рішень з протидії визначеним загрозам).

XDR поєднує в собі всі можливості EDR, UEBA, NTA, антивірусів наступного покоління та інших інструментів в одному рішенні, що забезпечує досягнення більш високих рівнів безпеки при скороченні загального часу реакції на інциденти. Це досягається завдяки забезпеченню комплексного контролю (сенсорики подій) та глибокої поведінкової аналітики в різних сегментах використовуваних мереж та ресурсів: - корпоративна локальна мережа; ресурси в хмарі та кінцеві точки.

4.1 Основні можливості XDR

XDR (Extended Detection and Response) — це платформа моніторингу ІБ, що забезпечує багатофакторний контроль та автоматичне реагування на інциденти не тільки на кінцевих точках, але і на набагато інших елементах корпоративної інфраструктури: від мобільних телефонів співробітників до хмарних додатків. Процес роботи зі складними інцидентами ІБ, що пов'язані з інтегральними загрозами безпеки та таргетованими атаками по цільовим елементами корпоративної інфраструктури [22], передбачає наявність автоматизованого процесу реагування, а точніше - виконання швидких і точних дій зі збирання потрібних відомостей, виявлення атипових мережевих ознак, аудиту телеметрії ІБ, та парирування відповідних загроз. Саме на цих завданнях і сфокусовані зусилля розробників XDR платформ (див. Рис. 4.1).

Як було зазначено вище, XDR- це еволюція EDR, яка забезпечує моніторинг та автоматичне реагування на кінцевих точках (наприклад, ноутбуки та робочі станції), але на теперішній час є багато інших точок вразливостей, які можуть бути під загрозою їх компрометації, починаючи від смартфонів персоналу і закінчуючи хмарними додатками та/або сервісами.

Важливо підкреслити, що технології *розширеного* виявлення та реагування мають ряд суттєвих переваг перед технологією *EDR*, а саме:

- підвищена швидкість виявлення загроз та реагування на них;

- збір та зіставлення даних зі значно більш широкого спектра джерел;

- забезпечення глибшого моніторингу загроз (робота з лог-файлами), що дозволяє суттєво мінімізувати можливі наслідки і масштаб атаки.

- об’єднання різнорідних завдань, вимог і параметрів функціонування всіх складових діючої системи безпеки, в межах єдиного стеку ІБ.

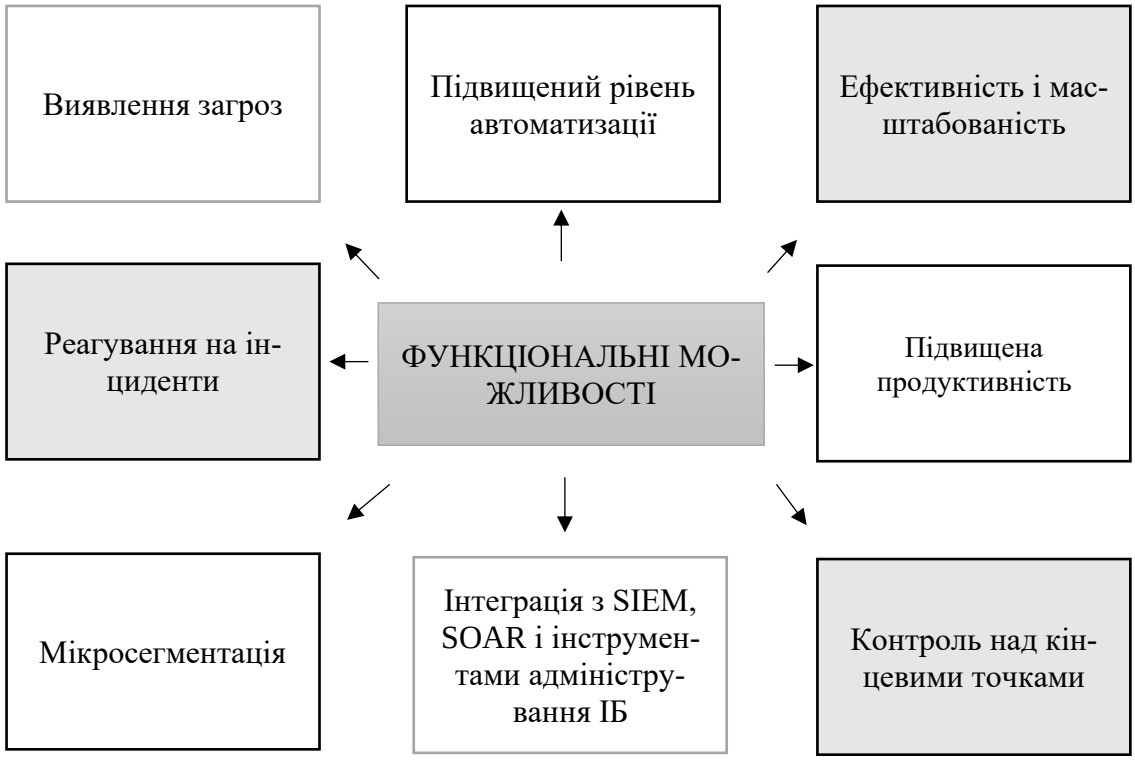


Рисунок 4.1 - Функціональні можливості XDR

Таким чином, *XDR* координує та «розширює цінність» окремих автономних інструментів ІБ, уніфікуючи і оптимізуючи аналіз поточного стану ІБ, забезпечуючи своєчасне усунення існуючих проблем безпеки (див. Табл. 4.1) [38].

Головний шлях до ефективного впровадження XDR – інтеграція. XDR повинен безперешкодно працювати у корпоративному стеку безпеки, використовуючи відносно прості інструменти з функціональним API. В цьому контексті важлива «глибина» готового функціоналу з кореляції подій, запобігання та реагування на атаки між наявними засобами захисту інформації (ЗЗІ). Іншими словами, вкрай важлива можливість дозволяти корпоративним аналітикам з питань ІБ, створювати та модифікувати свої власні міжстекові правила для виявлення та реагування на актуальні (для їх корпоративної інфраструктури та/або процесів) атаки. Синтезований для конкретних корпоративних структур (завдань) XDR, являє собою єдину платформу, яка дозволяє оперативно отримувати достатньо

інформативне уявлення про все, що відбувається в контрольованої мережі, з точки зору питань ІБ.

Таблиця 4.1 – Переваги XDR

Сутність переваг	Опис переваг
Консолідований інтегральний контроль загроз ІБ	*XDR* забезпечує багаторівневу та більш детальну ситуаційну поінформованість персоналу з ІБ.
Багатофакторне виявлення та аудит	*XDR* видаляє із потоку сповіщень ІБ, мережеві аномалії, які класифіковано як несуттєві. Завдяки використанню *AI* (*Artificial Intelligence*), *XDR* автоматично виявляє приховані загрози безпеки, що надає змогу персоналу сфокусуватися на аудиті критичних подій ІБ.
Наскрізне адміністрування та реагування	*XDR* забезпечує інтегровані автоматичні сповіщення та реалізує комплексні* зворотні дії реагування. * - *ініціює одночасний запуск складних робочих процесів з кількома інструментами безпеки (засобами) для нейтралізації, як точкових, так комплексних загроз.*

По-друге, важлива автоматизація, що підтримується штучним інтелектом та відповідними алгоритмами машинного навчання.

Т.ч., поєднання в межах XDR, функцій аналізу загроз, автоматизації і машинного навчання (*на базі впровадження технологій штучного інтелекту - AI*) допомагає компаніям оптимізувати продуктивність SOC, та зміцнити свою здатність знаходити та швидко реагувати на нові загрози. Зростання темпів впровадження XDR, перш за все, зумовлене його здатністю допомагати організаціям вирішувати дві важливі проблеми безпеки:

1) Виявлення та реагування на загрози, які постійно змінюють тактику та/або впроваджують нові способи обходу «традиційних» засобів ІБ. Так, традиційні системи SIEM, що стають дедалі складнішими та прихованими, важче виявляють невідомі техніки атак та експлойти [51,8], що створює потребу в запровадженні багатовекторних засобів безпеки, саме таких як є XDR;

2) Залучення досвідчених фахівців з ІБ в умовах широкого дефіциту навичок кібербезпеки, особливо у сфері аналізу загроз і аудиту ІБ [54].

4.2 Напрями створення XDR-систем

Існує два підходи до створення XDR-систем: - відкритий (Open XDR) та нативний (Native XDR).

Open XDR (також відомий як гібридний XDR) - стосується інтеграції сторонніх розробників/постачальників, а Native XDR - пропонує створення платформи за принципом «все в одному» (т.з., платформи від виробника). Кожен тип платформи XDR має переваги для різних випадків використання.

Open XDR не залежить від постачальника та забезпечує глибоку інтеграцію з найкращими у своєму класі інструментами від багатьох інших розробників (вендорів). Open XDR поєднує розширений аналіз і вміст, перевірений на місцях, із існуючими технологіями для зменшення складності, підвищення «видимості» подій і покращення управління ризиками в межах корпоративної ПІБ.

Гібридний підхід — це підхід до XDR, який інтегрує існуюче середовище безпеки користувача, включаючи всі його інструменти безпеки, як частину збору та аналізу даних. Відкритий XDR, на відміну від традиційних рішень XDR, які включають лише дані зі стеку власних технологій, призначений для отримання даних безпеки з усіх доступних джерел. Ці рішення часто використовують аналіз даних за допомогою штучного інтелекту (AI), щоб отримати більш інформативну та оперативну інформацію про поточний стан безпеки. Відкритий XDR використовує наявні в організації інструменти EDR або SIEM, поєднуючи відомості з локальних, хмарних і гібридних джерел. Він не призначений для заміни будь-якої конкретної технології, а натомість стоїть на верхньому рівні ієрархії існуючого стека безпеки (Звід правил) компанії, централізуючи вісь порядок збору, узагальнення і аналізу відповідних даних.

Відкриті рішення XDR призначені для агрегування, оптимізації та централізації процесу збору даних, що дозволяє заощаджувати кошти та покращувати системи ІБ. Сформулюємо перелік переваг гібридного XDR:

1) Централізовані дані безпеки розроблено для агрегування даних з усіх джерел безпеки, надаючи організаціям єдину платформу даних безпеки замість ручного поєднання інформації з різних джерел.

2) Спрощене виявлення та реагування, оскільки інформацію можна знайти в одному джерелі, тому персонал ІБ може легко виявити потенційного зловмисника або аномальну поведінку. Це значно пришвидшує час реакції, зменшуючи ризики та потенційну шкоду, яку може завдати атака ресурсів.

3) Можливість масштабованості дозволяє використовувати нові засоби безпеки та технології, а також підключатися до іншого відкритого рішення XDR. Оскільки відділ ІБ сучасних компаній постійно розширюється та впроваджуються нові технології, це ключова перевага, яку слід виділити.

4) Завдяки тому, що аналітики з питань безпеки мають єдину точку доступу через XDR, компанія може заощадити на ліцензіях та зменшити використання інших ресурсів.

5) Постійна оптимізація засобів безпеки, оскільки відкрите рішення XDR отримує дані безпеки в режимі реального часу, та можна, наприклад відстежити, чи існуючий інструмент припинив збір даних безпеки, або ж навпаки, видає помилкові спрацьовування. Це допомагає забезпечити безперервну роботу та оптимізацію технологій що використовуються.

Відкриті XDR, перш за все, підходять для організацій, що мають одразу кілька постачальників, розгорнутих у своєму IT-середовищі та середовищі безпеки. Програми безпеки, які є більш складнішими, і, як правило, використовуються у великих організаціях, котрі можуть мати більше ресурсів, потенційно можуть розгорнути найкращі у своєму класі інструменти ІБ від багатьох постачальників. Це може включати рішення EDR, SIEM та інші технології. У цьому випадку відкритий XDR вирішує те, що складно для наявного персоналу з ІБ – управління одразу кількома джерелами даних безпеки.

Відкриті XDR створені для ефективної інтеграції широкого спектру інших технологій у послідовну схему пошуку. Організації можуть раціоналізувати та розширити поточний набір інструментів, підвищивши їх «цінність» і

продуктивність, розмістивши відкритий XDR «поверх» наявного стека безпеки для централізації вимог щодо виявлення загроз, реагування та розслідування інцидентів. Групи безпеки, також можуть додавати нові інструменти та поєднувати та елементи від постачальників, отримуючи переваги від їх відкритого XDR.

Слід зазначити, що в результаті застосування відкритого (гібридного) підходу можна отримати рішення, яке просто встановити, але складно налаштувати та підтримувати. Обслуговуючий персонал може зіткнутися з такими труднощами: 1 - безліч методів та місць зберігання даних робить використання продукту незручним; 2 - набір інтеграцій із сторонніми рішеннями обмежений, а склад можливих рішень декларує виробник гібридного XDR; 3 - можлива втрата даних у процесі інтеграції.

Власні рішення XDR пропонують уніфікований набір інструментів безпеки від одного постачальника на платформі централізованого управління, яке має готову інтеграцію з додатковими некінцевими джерелами телеметрії, вбудованими в рішення та готовими до використання після налаштування. Це, теоретично, означає, що корпоративним командам з ІБ, не потрібно впроваджувати та керувати інтеграцією з технологіями інших постачальників. В свою чергу, це призводить до більш автоматизованого та спрощеного рішення для відділів безпеки завдяки моделі одного постачальника. Тому, головна перевага рішень нативних XDR полягає в наступному: - усі інтеграції та джерела телеметрії (спеціальних відомостей з ІБ) є частиною самого рішення, що дозволяє впровадити рішення, яке швидше розгортається, та вимагає меншого часу для оцінки поточного стану мережевої безпеки. До переваг нативних рішень XDR слід віднести наступні:

- єдина централізована платформа управління для адміністрування всіма процесами виявлення загроз і аналітики;

- не потрібно купувати, заново інтегрувати та оновлювати технології від інших розробників;

- висока готовність до інтеграції та швидшого розгортання.

Нативні XDR-системи найкраще підходить для організації з невеликими відділами та командами безпеки, тому що вони можуть використовувати додаткові джерела інформації про безпеку, в тому числі і внаслідок того, що їх персонал з ІБ має менше доступних ресурсів.

До недоліків слід віднести вимогу значної залежності від одного постачальника. Користувач, який вирішить скористатися власним рішенням XDR, повинен буде замінити наявні інструменти на інструменти з набору постачальника, що зазвичай є дорогим і складним процесом. Крім того, користувач, який віддає перевагу простоті підходу «все-в-одному», може зіткнутися із труднощами у виявленні загроз і реагуванні на них в діючий системі безпеки, оскільки один постачальник не в змозі забезпечити високій рівень безпеки в усіх сферах ІБ (векторах атак). Вибір цього підходу може вимагати пожертвування ефективністю захисту, якщо не всі рішення в пакеті постачальника є найкращими у своєму класі. Слід виділити такі недоліки нативних рішень XDR:

- залежність від одного постачальника платформи, через те, що перехід до іншого постачальника платформ є дуже довгим та коштовним;

- необхідність скопіювати та замінити існуючі інструменти безпеки – після підключення нативного рішення треба видалити всі вже встановлені рішення, через те, що ця платформа використовує свої інструменти безпеки;

- відсутність сторонніх можливостей інтеграції – використання вже готової платформи, що не підтримує можливість інсталяції рішень від інших розробників;

- низька адаптивність рішень – передбачає користування лише готовим рішенням, адже вся вибірковість налаштувань відключена (або блокована);

- неповні інтеграції – даний вид платформи підходить не до кожної системи, через що, не є універсальним рішенням для багатьох компаній;

- недолік захисту безпеки – є наслідком рідких оновлень складових компонентів системи, що викликане залежністю від одного постачальника послуг. Т.ч., можуть виникнути вразливості в діючий системі ІБ.

4.3 Принцип роботи XDR

Рішення XDR поєднують в себе ряд аналітичних засобів (інструментів) для виявлення загроз, які включають:

- аналіз внутрішнього та зовнішнього трафіку, який гарантує виявлення інсайдерів і скомпрометованих облікових даних, а також ідентифікацію зовнішніх атак. Відстежуючи та аналізуючи внутрішній і зовнішній мережевий трафік, XDR ідентифікує загрозу, навіть якщо вона вже оминула зовнішній периметр безпеки діючої системи;

- інтегрована розвідка про загрози - містить інформацію про відомі методи атак, інструменти, джерела та стратегії за різними напрямками атак. Розвідка загроз надає можливість XDR враховувати атаки на інші системи та використовувати цю інформацію для виявлення подібних подій в своєму середовищі [22];

- виявлення на основі машинного навчання - включає контрольовані та напівконтрольовані методи, які працюють для виявлення загроз на основі базових показників поведінки. Технології AI допомагають XDR виявляти загрози нульового дня, експлойти та нетрадиційні - таргетовані атаки, які можуть обійти методи на основі сигнатур [51,54,8].

В разі виявлення підозрілих подій, XDR надає інструменти, які допомагають персоналу визначити серйозність загрози та оперативно реагувати. Сформулюємо основні функції, які поєднують XDR та допомагають з розслідуванням і реагуванням на інциденти [54]:

- співвідношення пов’язаних попереджень і даних - інструменти автоматично групують пов’язані попередження, будують часові шкали атак із журналів активності та визначають пріоритет подій. Це допомагає визначити першопричину атаки та передбачити можливі дії зловмисника далі.

- централізований інтерфейс користувача - дозволяє аналітикам ІБ досліджувати події та реагувати на них з однієї консолі. Це пришвидшує час відповіді та спрощує документування відповідей.

- можливість модерації зворотної реакції системи захисту - реагування через інтерфейси XDR, а також інтегрування між інструментами. Наприклад: -

XDR оновлює політику «кінцевих точок» у відповідь на автоматично заблоковану атаку на одну з них.

Динамічне та гнучке розгортання XDR створене для реалізації переваг за часом. Нижче наведено деякі функції, які допомагають досягти цієї мети:

- адміністрування безпеки - можливість інтегрувати та використовувати існуючі елементи керування для уніфікованих і стандартизованих реакцій. Рішення XDR, також, містять функції автоматизації, які забезпечують послідовне розгортання політик безпеки для відповідних складових XDR і інструментів.

- масштабування сховищ даних та обчислювальної потужності - XDR використовує хмарні ресурси, які можна масштабувати відповідно до потреби в даних та проведення аналізу подій. Це гарантує, що дані, які корисні для виявлення та дослідження поточних загроз або інших тривалих атак, залишаються доступними.

- удосконалення з часом – використання можливостей AI гарантує, що рішення є ефективнішими у виявленні ширшого спектру атак з часом. У поєднанні з розвідкою про загрози, це допомагає забезпечити виявлення та запобігання максимальної кількості найбільш актуальних загроз.

Для забезпечення виявлення, розслідування, пошуку та реагування на інциденти ІБ, XDR рішення мають відповідати вимогам, котрі систематизовані в Табл.4.2.

Таблиця 4.2. – Вимоги до XDR

Перелік вимог	***Сутність вимог***
Робота на хмарній платформі	XDR працює в достатньому масштабі, маючи можливість отримувати дані з багатьох джерел, забезпечує широку видимість і можливості виявлення всіх даних і розташовується для оркестрування автоматизованої реакції.

Продовження Таблиці 4.2

Перелік вимог	***Сутність вимог***
Розширення безпеки кінцевої точки	XDR зосереджується на захисті кінцевих точок, але розширює видимість, виявлення та реагування за межі них завдяки інтеграції з рішеннями безпеки через схему відкритих даних.
Зосередження на загрозах	XDR автоматично виявляє приховані загрози, усуваючи необхідність створювати, налаштовувати та підтримувати правила виявлення, а також має широку, відповідну та розширену телеметрію. Він містить широкий, різноманітний набір систем і програм для більш повної контекстуалізації та кореляції, включаючи аналіз мережі та видимість, брандмауер наступного покоління, безпеку електронної пошти, ідентифікацію та керування доступом, захист робочого навантаження у хмарі, брокер безпеки доступу до хмари та інші.
Інтегрування з інструментами безпеки	XDR використовує відкриті, чітко визначені схеми для обміну даними з додатковими системами IT-безпеки, щоб забезпечити послідовне та комплексне збагачення та кореляцію з урахуванням ключових цілей і результатів.
Забезпечення змістовності розслідувань	XDR підкреслює точність даних і якість виявлення, щоб звести до мінімуму помилкові спрацьовування.
Прискорює реагування	XDR завдяки багатоплатформним робочим процесам реагування дає змогу командам безпеки вживати швидких (навіть автоматизованих) дій для усунення виявлених загроз.
Пошук прихованих загроз	XDR застосовує розширену аналітику безпеки, штучний інтелект і машинне навчання для безперервного пошуку раніше прихованих загроз, використовуючи агрегацію та розуміння кількох різнорідних слабкіших сигналів із різних доменів безпеки в стеку безпеки.

4.4 Аналіз найкращих XDR-платформ

Незважаючи на значний прорив у розвитку технологій безпеки за останній час, труднощі, з якими стикаються фахівці з ІБ, намагаючись впоратися з потоком повідомлень про порушення, що постійно зростає, тільки загострюються. Так, фактично більше ніж 77% фахівців з ІБ [35] наголошують на те, що виявляти та реагувати на загрози стає все складніше.

Перш ніж вибрати послугу XDR, слід попрацювати із «зацікавленими» сторонами, щоб вирішити, чи э обрана стратегія XDR достатньою для даної організації. При цьому слід враховувати і таки опосередковані фактори, як рівень обізнаності персоналу його продуктивність (у контексті професійних якостей), бюджет безпеки тощо. Необхідно провести ретельну оцінку та тестування продукту, щоб гарантувати, що результати будуть такими, як очікуються. Рішення XDR повинно дозволити персоналу з ІБ своєчасно запобігати, виявляти, досліджувати та усувати загрози в межах діючої платформи. Крім того, вкрай важливо щоб XDR рішення включало до свого складу, ряд додаткових інтегрованих інструментів, наприклад: - збір телеметрії з низки джерел (включно з кінцевими точками, електронною поштою, мережами, серверами, ідентифікацією тощо); консолідацію пов’язаної інформації в більш доступному вигляді, інформативні але при цьому й легковажні сповіщення ІБ; визначення пріоритетів за допомогою AI; автоматизацію робочих процесів, щодо формування сповіщень системи безпеки та логування подій.

Дані електронної пошти, кінцевих точок, серверів, хмарних процесів і телеметрія мережевої активності, збирається та співвідноситься, щоб забезпечити наочність відображення поточного стану та змісту розширених загроз, що детектуються. Втрату даних і порушення безпеки можна запобігти шляхом аналізу, визначення пріоритетів, пошуку та усунення загроз. Тому XDR одночасно забезпечує функціональність централізації та нормалізації даних в базах даних цієї системи для наступних аналізу та запитів. Інструмент XDR повинен мати відповідні можливості реагування на інциденти безпеки, щоб змінити стан окремого

продукту безпеки як частину процесу відновлення, а також має забезпечити покращення показників виявлення загроз.

На сьогоднішній день ринок XDR стрімко розвивається, тому важливо визначити, основні властивості і можливості існуючих рішень. Для цього були проведені відповідні аналітичні дослідження та визначено низку найкращих рішень XDR, що є на ринку ІБ, включаючи огляд їх ключових функцій та пропозицій, стосовно умов функціонування для яких вони найкраще підходять.

4.4.1 Palo Alto Networks Cortex XDR

Компанія Palo Alto Networks є світовим лідером у сфері корпоративних рішень для кібербезпеки. Вона створила перший у галузі продукт XDR - Cortex XDR. Cortex XDR доступний у двох версіях, Prevent та Pro [31]:

- Cortex Prevent - забезпечує захист кінцевих точок і включає функції контролю пристроїв, шифрування диска та брандмауера хоста. Він також включає механізм інцидентів, інтегровані можливості реагування та додатковий канал розвідки про загрози.

- Cortex Pro - забезпечує той самий захист, що й Prevent, але для кінцевих точок, мереж, хмарних ресурсів і продуктів сторонніх розробників. Він також містить функції для аналітики поведінки, виявлення на основі правил, прискореного розслідування та додаткового керованого пошуку загроз (Рис.4.2).

Архітектура Cortex XDR дещо відрізняється між версіями продукту, але включає кілька стандартних компонентів. Обидва видання покладаються на Cortex Data Lake і розроблені для кореляції даних журналу на пристроях.

Основні компоненти платформи включають:

-Додаток Cortex XDR — інтерфейс користувача (UI- User Interface), який забезпечує видимість Data Lake. За допомогою цього інтерфейсу користувача можна сортувати та досліджувати сповіщення, вживати заходів для виправлення та визначати власні політики виявлення та реагування.

-Cortex Data Lake - ресурс зберігання для хмарного журналювання, призначений для зберігання даних журналу з усіх джерел. Озеро даних централізує дані, дозволяючи механізму XDR корелювати події та створювати сповіщення.

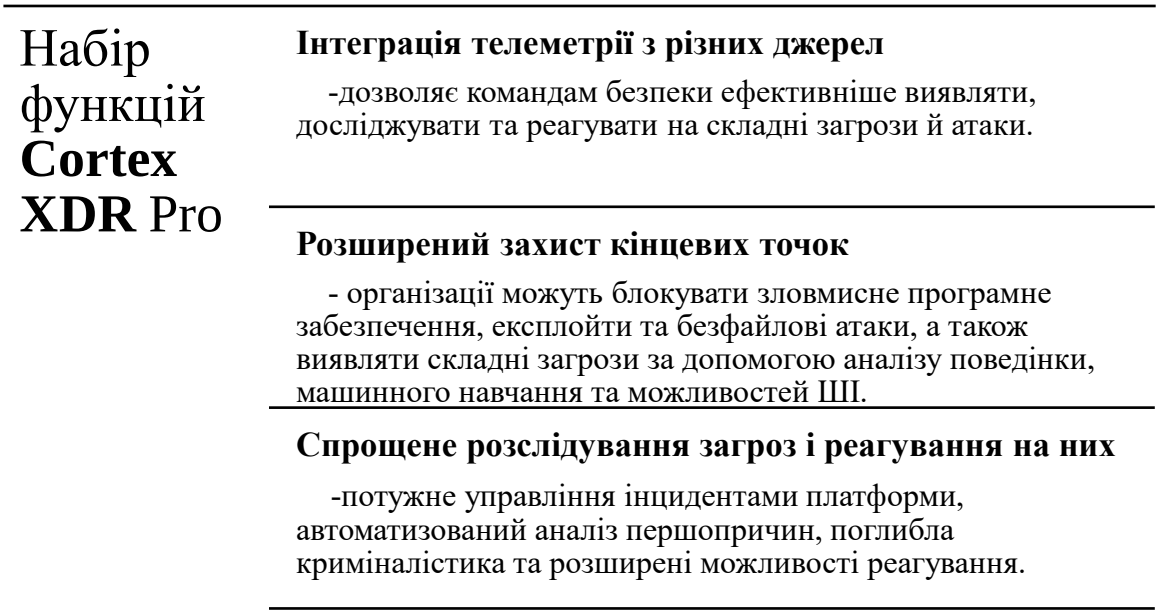


Рисунок 4.2 – Ключові можливості Cortex XDR Pro

Розширені компоненти платформи включають [31]:

1) Механізм аналітики — служба безпеки, яка використовує дані мережі та кінцевих точок для виявлення загроз і реагування на них. Він застосовує аналітику поведінки для виявлення як відомих, так і невідомих загроз шляхом порівняння з відомою та прийнятною поведінкою користувачів або пристроїв.
2) Брандмауери наступного покоління — віртуальні або локальні брандмауери, які можна використовувати для застосування політик безпечного трафіку у вашій мережі. Ці брандмауери містять технології машинного навчання, які допомагають виявляти відомі та невідомі загрози.
3) Prisma Access і GlobalProtect — служби, за допомогою яких можна розширити захист брандмауера для віддалених і мобільних користувачів. Ці служби дають змогу пересилати віддалені журнали трафіку до озера даних, щоб забезпечити спільну кореляцію з локальними журналами.
4) Зовнішні брандмауери та сповіщення — завдяки інтеграції можна завантажувати журнали зовнішнього брандмауера та сповіщення у свою систему Cortex XDR. Це можливо через Cortex XDR API. Потім ці точки

даних можна поєднати з даними Cortex, щоб надати більше контексту для подій і забезпечити більш ретельну відповідь.

5) Агенти Cortex XDR — програмне забезпечення, встановлене на кінцевих точках, яке використовується для збору та пересилання даних. Ці агенти також можуть виконувати локальний аналіз і використовувати інформацію про загрози WildFire для покращеного виявлення загроз. Усі зібрані дані також надсилаються в Data Lake для спільного аналізу.

Користувачі високо оцінюють Cortex XDR за його розширені можливості дослідження, детальну аналітику інцидентів та легку інтеграцію з іншими продуктами Palo Alto Networks. Однак при цьому користувачі відзначають достатню кількість помилкових спрацьовувань.

Оцінюючи можливості цього рішення та узагальнюючи відгуки її користувачів, можна стверджувати, ця XDR більш підходить для середніх організацій, яким потрібне потужне, добре налагоджене рішення XDR, а також для існуючих клієнтів тієї ж самої Palo Alto Networks, які хочуть розвивати свої існуючі інструменти (наприклад, Cortex XSOAR).[43]

4.4.2 Cynet

Cynet - це автономна платформа захисту від злому, яка забезпечує вбудовану інтеграцію NGAV (Next Generation Antivirus), EDR, UEBA, аналізу мережевого трафіку та обману (пастки – аналогу HPot [21]) для виявлення та усунення загроз, а також широкий спектр можливостей автоматизованого виправлення за допомогою технології Sensor Fusion для постійного збору та аналізу активності «кінцевої точки», діяльності користувачів та мережі в усьому корпоративному середовищі. Він здійснює постійний моніторинг кінцевих точок. Це допоможе виявити активну шкідливу присутність і приймати швидкі та ефективні рішення щодо її масштабу та впливу. Крім того, є можливість автоматичного запобігання виконання зловмисного коду та використовуються макроси сценаріїв. Основні можливості які реалізує Cynet, представлені в Табл.4.3.

Таблиця 4.3 — Основні можливості Cynet

Функція	***Сутність реалізації***
Захист кінцевої точки	*Багаторівневий захист від шкідливих програм, програм-вимагачів, експлойтів і атак без файлів.*
Захист мережі	*Захист від атак сканування, MITM (Man-In-The-Middle), бокового переміщення та викрадання даних.*
Захист користувачів	*Попередньо встановлені правила поведінки в поєднанні з динамічним профілюванням поведінки для виявлення зловмисних аномалій.*
Обман (*пастка***)**	*Широкий набір мережевих, користувацьких і файлових приманок, щоб спонукати «досвідчених» зловмисників до виявлення їх прихованої присутності.*

Cynet розгортається на тисячах кінцевих точок менш ніж за дві години. Він використовується для виявлення складних загроз, а потім виконується автоматичне або ручне виправлення, знешкоджуючи зловмисну діяльність, та мінімізуючи шкоду, спричинену атаками [35].

Cynet виявляє та запобігає атакам, які включають скомпрометовані облікові записи користувачів. Він використовує метод обману, щоб виявити присутність зловмисників шляхом встановлення підроблених паролів, файлів даних, конфігурацій і мережевих з'єднань. Він має функції для запобігання та виявлення мережевих атак. Для моніторингу та контролю він пропонує такі функції, як керування активами та оцінка вразливості. Як узгодження відповіді, він може виконувати ручні та автоматичні дії з відновлення файлів, користувачів, хостів і мережі. Сформулюємо функції, які користувачі вважають найбільш цінними в даному рішенні [42]:

1) Cynet може швидко відобразити всю IT-інфраструктуру ,скануючи активи, включаючи кінцеві точки, користувачів, файли та мережевий трафік, щоб відобразити інформаційну панель проблем безпеки.
2) Запобігання: різноманітні можливості запобігання включають UBA, обман і традиційний захист кінцевої точки.

3) Виявлення: це включає в себе традиційну безпеку кінцевих точок, EDR, UBA, обман і мережеву аналітику, яка допомагає виявляти зловмисну поведінку, програми-вимагачі, експлуатацію, аномалії входу користувачів, тунелювання DNS і багато іншого.
4) Керування вразливістю: Cynet може знаходити вразливості ПЗ, неавторизовані та застарілі програми та порушення політики безпеки.
5) Відповідь: Cynet включає різноманітні можливості аналізу, реагування та виправлення для кінцевих точок, файлів, користувачів і мереж.
6) Автоматизована відповідь: користувачі можуть створити автоматичне правило виправлення для кожного сповіщення, створеного Cynet, що допомагає покращити процес реагування на інцидент і може запобігти загрозі в реальному часі.
7) Неперервність технічної підтримки: - Cynet включає цілодобову операційну команду, доступну для їх користувачів у будь-який час.

Отже, Cynet надає єдину платформу для захисту організації шляхом автоматизації моніторингу та контролю, запобігання та виявлення атак, а також оркестрування відповіді. Це єдина платформа, яка інтегрувала можливості NGAV (Next Generation Antivirus), EDR, NTA, UEBA та Deception. Це рішення отримало найвищі оцінки від користувачів за легкість розгортання та ефективне спілкування. За сукупністю характеристик та властивостей, Cynet ована підходить великим корпоративним системам або крупним організаціям, що мають невеликий персонал ІБ.

4.4.3 CrowdStrike Falcon XDR

CrowdStrike Falcon XDR - це рішення XDR, розроблене для розширення щодо виявлення та реагування на кінцеві точки (EDR), та збирання між інструментами телеметричні дані. Рішення також може аналізувати загрози в кількох доменах, а також забезпечувати організовану відповідь — усе з однієї уніфікованої платформи.

Falcon XDR корелює події та телеметрію між кінцевими точками, хмарою, інструментами ідентифікації та сторонніми інструментами, створюючи єдиний

пріоритетний потік сповіщень. Тоді платформа може автоматично виявляти будь-які загрози та проводити розширене розслідування за допомогою відображення та візуалізації MITER ATT&CK, допомагаючи командам безпеки краще розуміти їх і реагувати на них. Тоді платформа спрощує реагування, надаючи потужну аналітику та аналіз основних причин, стримування підозрілої активності та автоматичні робочі процеси реагування .[42]

CrowdStrike Falcon XDR надає такі ключові можливості:

- розширене виявлення та реагування в різних середовищах. Користувачі можуть оптимізувати виявлення загроз у реальному часі, розслідування та пошук у різних середовищах і доменах за допомогою безперебійного прийому та кореляції найрелевантнішої телеметрії безпеки.

- візуалізовані контекстні виявлення в різних доменах. Забезпечує швидкі та прості дослідження та створює спеціальні сповіщення про поведінку та дії, унікальні для кожного клієнтського середовища.

- покращена ефективність і результативність. Усуває операційну неефективність різнорідних інструментів і рішень шляхом тісної інтеграції з існуючими рішеннями користувача для створення цілісного та більш ефективного стека кібербезпеки.

- прискорене реагування повного циклу. Прискорення дій реагування, дозволяючи користувачам організовувати й автоматизувати будь-який робочий процес безпеки, створюючи можливості активного сповіщення та реагування в реальному часі разом із настроюваними тригерами на основі виявлення та категоризації інцидентів.

Оскільки Falcon XDR побудовано на розширенні можливостей EDR CrowdStrike, платформа добре підходить для поточних користувачів EDR, які хочуть розширити своє рішення в XDR, а також для організацій, які мають велику кількість кінцевих точок для захисту. Це рішення можна рекомендувати для підприємств, які шукають потужне рішення XDR для забезпечення цілісного захисту від загроз і можливостей швидкого реагування, які виходять за межі «кінцевої точки».

4.4.4 Особливості визначення найкращого рішення XDR для різних організацій

Основою стратегії безпеки будь-якої організації має бути підхід, спрямований на запобігання. Що стосується невідомого зловмисного програмного забезпечення, захист від поведінкових загроз. Cortex XDR і аналіз на основі штучного інтелекту перевершують CrowdStrike та Cynet як у реальних оцінках, так і в тестуванні. Відстежуючи послідовність ланцюжка дій і застосовуючи контекст до цих дій, коли вони відбуваються, захист від поведінкових загроз здатний автоматично й точно розпізнавати та запобігати складним атакам із високим ступенем ухилення. Cortex XDR у поєднанні із запобіганням експлойтам на основі техніки, глобальним аналізом загроз і хмарним аналізом забезпечує найкращий і надійніший захист.

Покладення CrowdStrike на захист на основі хешування зосереджується лише на відомих атаках і виявленні постфактум, тому захист страждає, про що свідчить нездатність зупинити 30% атак.[50]

Що стосується виявлення та «видимості», Cortex XDR перевершує CrowdStrike та Cynet. Широкий перелік даних телеметрії Cortex та розширені модулі виявлення хмарної аналітики, виявляють недекларовану поведінкову та/або мережеву активність протягом всього життєвого циклу атаки, та мають дані, необхідні для вирішення цієї проблеми. Ці можливості Cortex, стосовно аналітики і виявлення, перевершують CrowdStrike та Cynet, тому що останні рішення детектують меншу кількість виявлень аналітики, зі значною кількістю відкладених виявлень. Затримки в такому ділі, можуть мати значні наслідки для безпеки, адже можливість виявлення в реальному часі означає і швидший час реакції, та відповідно менші наслідки для організації (установи).

Cortex XDR автоматично групує сповіщення в інциденти, забезпечує моделювання загроз, збирає повний контекст і створює часову шкалу та послідовність атак, щоб зрозуміти першопричину та наслідки атаки. Дослідження користувачів показують, що Cortex XDR може зменшити сповіщення системи безпеки на понад 98% і скоротити час дослідження на 88%.[31]

В цілому, CrowdStrike потребує значно уваги від персоналу для розслідування та відновлення системи після атак. Події представлені окремо, відповіді виконуються індивідуально, а виправлення виконується вручну та мають обмежену автоматизацію. Притаманні більший ризик, менша ефективність і затримка відновлення. Загальне порівняння цих 3-х рішень представлено у Табл.4.4

Таблиця 4.4 - Порівняльна характеристика рішень XDR

Завдання	***Cortex XDR***	***CrowdStrike***	***Cynet***
Захист	*100% запобігання загрозам та загальна активна профілактика; *включає механізм програм-вимагачів, локальний аналіз на основі ШІ та захист від поведінкових загроз для запобігання складним та обхідним атакам; *вбудований брандмауер кінцевої точки, контроль пристроїв та аналіз виявляють нові загрози та автоматично розповсюджують оновлення.	*70% захисту, адже 30% атак не вдається зупинити та є пропуски захистів; *відсутність захисту від поведінкових загроз та залежності від статичного хеш-аналізу; *обмежені режими запобігання з брандмауером кінцевої точки та контролем пристроїв доступні лише як кошотовні додаткові функції.	*80% захисту, адже 20% атак не вдається зупинити та є пропуски захистів; *використання однієї ліцензії, що дозволяє кінцевим користувачам отримати усі функції для захисту кінцевої точки; *функції включають NTA , UBA , NGAV, EDR і MDR.

Продовження Таблиці 4.4

Завдання	***Cortex XDR***	***CrowdStrike***	***Cynet***
Виявлення	*98,2% аналітичного охоплення та виявлення на рівні техніки; *широкий збір даних та аналіз даних за допомогою ШІ забезпечують швидке й точне виявлення *нові правила виявлення аналізують як нові, так й історичні дані для повної видимості.	*неповна видимість та пропущені виявлення; *машинне навчання вузько орієнтоване на події та журнали, пов'язані з ідентифікацією також доступне за додаткову плату; *історичні дані виключено з області нових правил виявлення.	*розширене виявлення та захист від програм-вимагачів у поєднанні з моніторингом SOC; * нові дані неправильно сприймається продуктом, і не виконуються всі необхідні дії;
Розслідування та реагування	*автоматична кореляція подій дозволяє аналітикам бачити інцидент, а групування попереджень та оцінювання інцидентів скорочують час розслідування на 88%; *виправлення можна зробити за допомогою однієї дії, що дозволяє службам реагування швидко відновлюватися після інцидентів.	*кожна подія представлена окремо, що вимагає більше зусиль та часу для аналізу та визначення масштабу інциденту; *відсутність автоматизованих завдань означає, що час витрачається аналітиками, які повинні реагувати індивідуально та вручну.	*автоматизація на достатньому рівні, тому що в більшості випадків він блокує атаки, не вимагаючи дій від аналітиків; *аналіз поведінки користувачів у мережі та аналіз мережі для команди безпеки;

Продовження Таблиці 4.4

Завдання	***Cortex XDR***	***CrowdStrike***	***Cynet***
Належність до організацій	*дані надходять з будь-якого системного журналу, журналу подій, файлів або джерел на рівні організації; *XDR включає захист кінцевих точок та повністю надається через єдиний уніфікований агент; *правила виявлення та інформаційні панелі легко налаштовуються відповідно до потреб кожної організації;	*дані за межами кінцевих точок надаються лише партнерами CrowdStrike; *підвищення складності; *мінімальні параметри налаштування	*конфігурація та використання продукту досить проста; *інтерфейс користувача незручний; *щоденне робоче навантаження приблизно дорівнює нулю, а також краща видимість, оскільки не потрібно переходити від екрана до екрана.

В цілому, Cortex XDR лідирує за загальним показником запобігання та виявлення загроз (див. Рис.4.3).

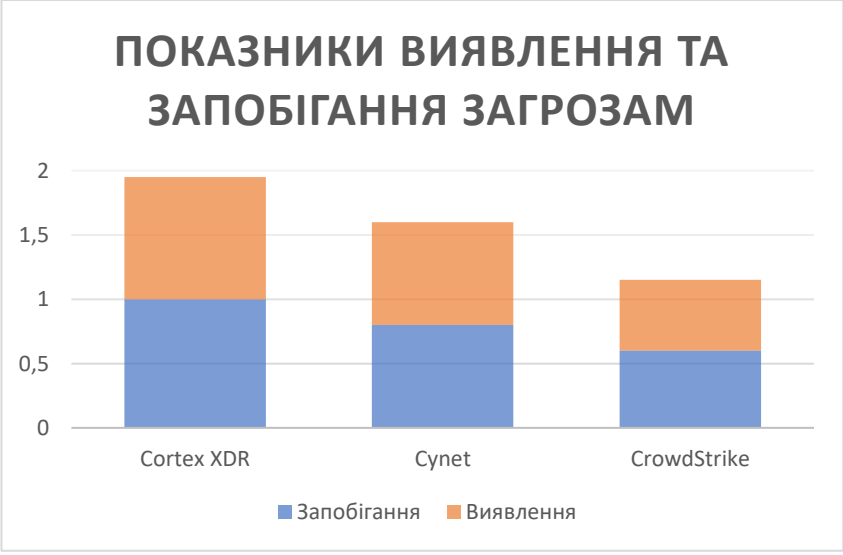


Рисунок 4.3 – Дані MITRE ATT&CK Engenuity 2021 рік [43]

Тестування виявлення атак, а також перевірка можливостей щодо запобігання атакам, в якій оцінювалися можливості СЗІ блокувати атаки на кінцевих

точках, свідчить, що рішення Palo Alto Networks володіє ефективними технологіями для запобігання сучасним загрозам ІБ та широким функціоналом захисту для кінцевих точок. Це рішення блокує всі відомі атаки на Linux і Windows, і при цьому демонструє найбільшу кількість детектів (спрацювань), підтверджуючи найкращу якість серед інших вендорів із запобіганням загроз (100%).

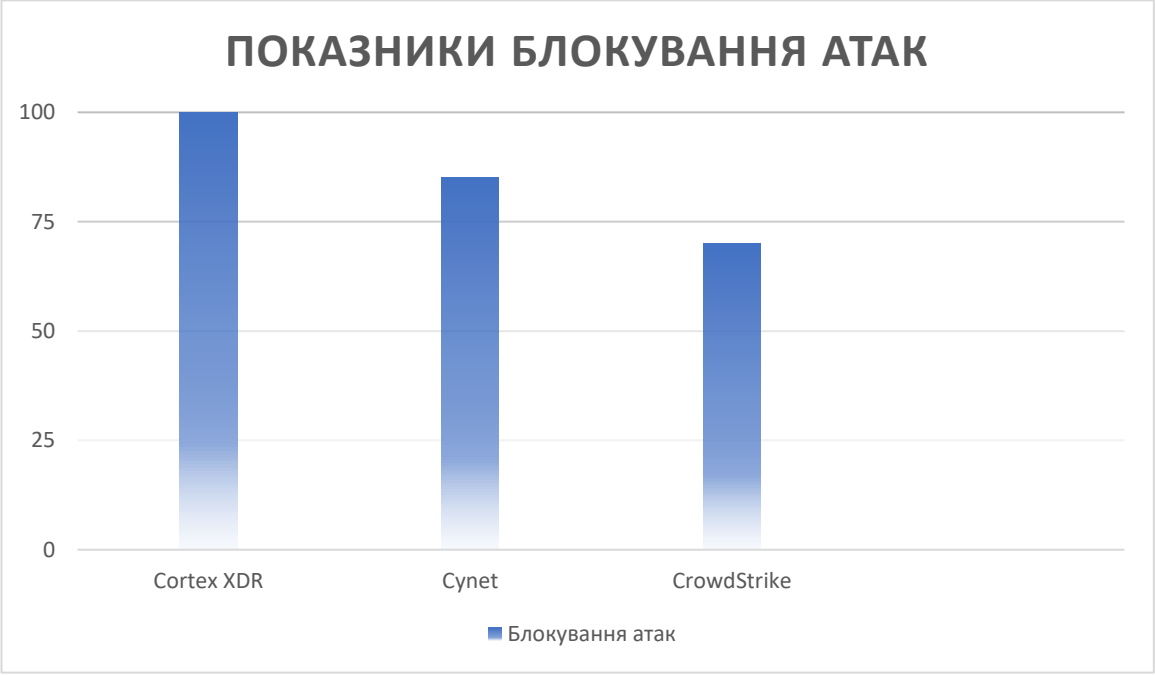


Рисунок 4.4 – Дані MITRE ATT&CK Engenuity 2021 рік [43]

Також слід зазначити, що Cortex XDR перевершує за рівнем моніторингу серед інших рішень із показником захисту 100%.

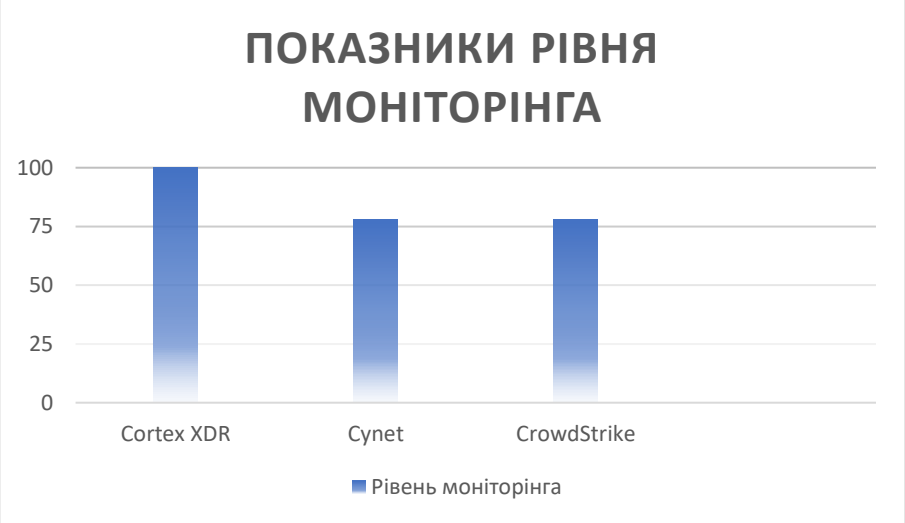


Рисунок 4.5 – Дані MITRE ATT&CK Engenuity 2021 рік [43]

Отже, Cortex XDR не тільки запобігає атакам у перевірках можливостей захисту, але й використовує дані лог-файлів з міжмережевих екранів нового покоління (рівня *Next Generation Firewall (NGFW)*), завдяки чому підвищується точність виявлення загроз. Т.ч., Cortex збирає та інтегрує відомості про кінцеві точки та мережі, що забезпечує достатньо глибокий моніторинг поточної активності.

Сучасні мережеві зловмисники найчастіше атакують керовані «кінцеві точки», проте можуть атакувати і некеровані, а також хмарні додатки, та навіть мережеве обладнання (комутатори, шлюзи, накопичувачі даних тощо) і безпосередньо засоби захисту (наприклад, той же самий Honeypot). Тому службам ІБ вкрай важливо реалізувати комплексний підхід, який не обмежується тільки рамками традиційних EDR-рішень, а дозволяє вести моніторинг поточних подій у масштабі всієї організації. В цьому сенсі, Cortex XDR дає можливість блокувати сучасні атаки, залучаючи для цього аналітику накопичених логів з хмарних активів, кінцевих точок та різнорідних мережевих пристроїв, що входять до периметру безпеки цієї XDR. На сьогоднішній день це рішення демонструє достойні уваги результати в тестуванні загроз, завдяки комбінації високоінформативних даних та глибокої поведінкової аналітики.

ВИСНОВКИ

В роботі досліджено можливості та специфіку реалізації XDR-технології, як засобу комплексної протидії актуальним загрозам ІБ, що притаманні корпоративному сегменту ІТ- ринку. Розглянуто сучасні погляди на вирішення існуючих труднощів при експлуатації існуючих систем безпеки (перш за все на рівні EDR та SIEM- систем), та визначені передумови для впровадження XDR рішень для захисту корпоративних інформаційних ресурсів. Розглянуто особливості впровадження XDR технології, як в контексті питань забезпечення вимог корпоративних політик ІБ, так в контексті проблематики протистояння впливу сучасних загроз. За результатами проведеного аналізу визначені особливості визначення «найкращих» варіантів реалізації відповідних XDR рішень, що враховують специфіку різних організацій.

Підкреслено, що одна з основних переваг XDR рішення, це підвищення ефективності роботи персоналу (фактично вирішення проблем кінцевого аудиту подій та прийняття рішень в випадках, які складно формалізуються) за рахунок автоматизації виявлення і реагування на переважну більшість інцидентів.

Звернено увагу, на той факт, що у XDR є кілька особливостей, що дають інтегрований ефект, та сприяють підвищенню фактичного рівня захисту:

- незалежність від елементів управління;

- можливість інтеграції з кількома іншими технологіями, що не потребує прив’язки до його (XDR) постачальника;

- потужні можливості автоматичної кореляції подій та виявлення мережевих і поведінкових аномалій (з залученням AI);

- швидкий, багатовекторний аналіз і логування мережевих подій за багатьма типами датчиків, що зменшує кількість помилкових спрацьовувань;

- використання попередньо створених моделей даних за різними типами та/або сегментами відомих мережевих структур;

- інтегрування функцій мережевої розвідки (про загрози) та виявлення і реагування на інциденти ІБ, без потреби постійного втручання персоналу, для випадків типових (що корелюють) сигнатур атак, що виключає необхідність залучення персоналу для коригування відповідних правил.

Підкреслено, що спряження XDR з SIEM, SOAR та інструментами управління процесами ІБ, дозволяє компаніям максимізувати вартість своїх інвестицій, замість того, щоб вимагати заміни існуючих (працюючих) рішень ІБ. При цьому персонал з ІБ своєчасно та безперервно інформується про ефективність роботи наявний складових, в межах корпоративного стеку безпеки, де безумовно існують певні «слабкі місця», та які кроки потрібно вжити для усунення визначених вразливостей в діючої системі безпеки. Тобто використання XDR дозволяє в значній мірі скоротити час реакції персоналу ІБ на формування ефективного захисту в умовах постійної появи (пресингу) нових загроз.

Визначено, що ринок XDR стрімко розвивається, тому важливо визначити, основні властивості і можливості існуючих рішень, серед яких, станом на сьогоднішній день, слід особо виділити Cortex XDR, який лідирує за загальним показником запобігання та виявлення відомих загроз, а також перевершує за рівнем моніторингу, серед інших рішень, із показником захисту майже 100%.

Отже, поява XDR, є результатом еволюції інструментів виявлення і реагування на інциденти ІБ , що не обмежується рівнем кінцевих точок (EDR). Існуючи XDR платформи поєднують в собі основні можливості EDR, UEBA, NTA та антивірусів покоління Next. Така інтеграція досягається завдяки забезпеченню комплексної видимості та глибокої поведінкової аналітики (включаючи корпоративну мережу, «свої» ресурси в хмарі та кінцеві точки). Впровадження XDR-рішень прискорює розслідування інцидентів та використовує широку автоматизацію для збільшення ефективність роботи наявного штату фахівців ІБ.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Social Engineering: The Art of Human Hacking / Christopher Hadnagy. – Wiley Publishing, Inc., 2010. 416 с.
2. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Київ: ДУТ, 2015. 288 с.
3. Угрозы информационной безопасности. URL: http://surl.li/ukfa (дата звернення: 22.05.2021).
4. Понятие информации. Раздел 1. Общие вопросы защиты информации. URL: http://surl.li/ukgs (дата звернення: 22.05.2021).
5. Скиба В.Ю. Руководство по защите от внутренних угроз информационной безопасности / В.Ю. Скиба, В.А. Курбатов. – СПб.: Питер, 2008. – 320 с.
6. Погоріла К.В. Передумови, способи реалізації та протидія інсайдерським загрозам в сучасних умовах. Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: матеріали 11-ї міжнар. наук.-техн. конф., (Т.2, с. 67). 8-9 квітня, 2021, Харків, Україна. Вилучено з: http://repository.kpi.kharkov.ua/handle/KhPI-Press/52020.
7. Исследование утечек информации ограниченного доступа в 2019 году. URL: https://www.infowatch.ru/analytics/reports/27720 (дата звернення: 13.03.2021).
8. Погоріла К.В. (2021) Аналіз та дослідження технологій соціального інжинірингу при реалізації протидії інсайдерським загрозам (дипломна робота бакалавра). ХНУ ім. В.Н. Каразіна, Харків, Україна.
9. Шипкова Н. (2022).Как оценить и развернуть XDR платформу URL: https://www.securitylab.ru/analytics/529176.php (дата звернення: 10.09.2022).

10. Блог «Тайгер Оптикс». (2021). Что такое XDR? (и зачем он нужен). URL: https://blog.tiger-optics.ru/2021/03/xdr/ (дата звернення: 10.09.2022).
11. Яна Шевченко. (2021). XDR: новая стратегия повышения эффективности защиты от кибератак. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/XDR-as-new-strategy-to-improve-cyber-attacks-protection (дата звернення: 11.09.2022).
12. Дідух Т.М. Глобальні ризики використання it-аутсорсингу. Вісник Миколаївського національного університету імені В.О. Сухомлинського. Вип. 20. 2017. С. 28-32.
13. Погоріла К.В., Гайкова В.В. Прийоми соціальної інженерії та шляхи протидії її проявам в сучасних інформаційних системах. Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: матеріали 11-ї міжнар. наук.-техн. конф., (Т.2, с. 67). 8-9 квітня, 2021, Харків, Україна. Вилучено з: http://repository.kpi.kharkov.ua/handle/KhPI-Press/52020.
14. Безопасная сеть вашей компании / Джон Маллери, Джейсон Занн и др.; пер. с англ. Е. Линдеманн. – М.: НТ Пресс, 2007. 640 с.
15. Что такое XDR. URL: https://www.trendmicro.com/ru_ru/what-is/xdr.html (дата звернення: 13.09.2022).
16. Endpoint Detection & Response (EDR) URL: https://encyclopedia.kaspersky.ru/glossary/edr-endpoint-detection-response/ (дата звернення: 14.09.2022).
17. Що таке виявлення та відповідь кінцевої точки (EDR)? URL: https://www.cisco.com/c/en/us/products/security/endpoint-security/what-is-endpoint-detection-response-edr-medr.html (дата звернення: 15.09.2022).
18. WHAT IS ENDPOINT DETECTION AND RESPONSE (EDR).(2021) URL: https://www.crowdstrike.com/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/ (дата звернення: 15.09.2022).

19. Anne Aarness. (2022). WHAT IS XDR? URL https://www.crowdstrike.com/cybersecurity-101/what-is-xdr/ (дата звернення: 16.09.2022).
20. What Is Endpoint Detection and Response (EDR)? URL: https://www.trellix.com/en-us/security-awareness/endpoint/what-is-endpoint-detection-and-response.html (дата звернення 18.09.2022).
21. Мелкозьорова О.М., Погоріла К.В. Особливості синтезу поведінкових профілів Honeypot/ Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: матеріали 11-ї міжнар. наук.-техн. конф., (Т.2, с. 67).8-9 квітня, 2021, Харків, Україна.
Вилучено з: http://repository.kpi.kharkov.ua/handle/KhPI-Press/52020.
22. Особливості захисту корпоративних ресурсів за допомогою технології Honeypot. / Погоріла, К.В. та ін. (2020). Комп'ютерні науки та кібербезпека, (4), С.22-29.
https://doi.org/10.26565/2519-2310-2019-4-03
23. Что такое SIEM-системы и для чего они нужны? URL: http://surl.li/ukgo (дата звернення: 18.09.2022).
24. Why is SIEM important? URL: https://www.ibm.com/topics/siem (дата звернення: 20.09.2022).
25. What is user and entity behavior analytics? (UEBA) URL: https://www.rapid7.com/fundamentals/user-behavior-analytics/ (дата звернення: 22.09.2022).
26. Chris Brook . (2020) What is User and Entity Behavior Analytics? A Definition of UEBA, Benefits, How It Works, and More URL: (дата звернення: 22.09.2022).
27. What Is SOAR? URL: https://www.paloaltonetworks.com/cyberpedia/what-is-soar (дата звернення: 23.09.2022).
28. Что такое network traffic analysis и зачем нужны NTA-системы. (2019). URL: https://www.ptsecurity.com/ru-ru/research/knowledge-base/chto-takoe-

network-traffic-analysis-i-zachem-nuzhny-nta-sistemy/ (дата звернення: 24.09.2022).

29. Hossein Ashtari .(2022) What Is Network Traffic Analysis? Definition, Importance, Implementation, and Best Practices. URL: https://www.spiceworks.com/tech/networking/articles/network-traffic-analysis/ (дата звернення: 24.09.2022).
30. Incident Response Automation and Security Orchestration with SOAR. URL: https://www.exabeam.com/explainers/siem/incident-response-and-automation/ (дата звернення: 25.09.2022).
31. Cortex XDR by Palo Alto: Architecture & Capabilities Overview. URL: https://www.cynet.com/xdr-security/xdr-by-palo-alto-understanding-cortex-xdr/ (дата звернення: 25.09.2022).
32. Джон Маллери, Джейсон Занн (2007). *Безопасная сеть вашей компании.* (Е. Линдеманн, пер. с англ.). Москва: НТ Пресс.
33. XDR and its Components Explained —Open XDR vs. Native XDR. (2022). URL: https://hackernoon.com/xdr-and-its-components-explained-open-xdr-vs-native-xdr (дата звернення: 25.09.2022).
34. Современные технологии защиты от утечки конфиденциальной информации. URL: https://searchinform.ru/analitika-v-oblasti-ib/utechki-informatsii/prichiny-utechki-informatsii/istochniki-utechki-informacii/utechka-konfidencialnoj-informacii/sovremennye-tekhnologii-zashchity-ot-utechki-konfidencialnoj-informacii/ (дата звернення: 30.09.2022).
35. 10 Best XDR Solutions: Extended Detection And Response Services In 2022. URL: https://www.softwaretestinghelp.com/xdr-security-solutions/ (дата звернення: 30.09.2022).
36. Understanding Open XDR. URL: https://www.exabeam.com/explainers/xdr/understanding-open-xdr/ (дата звернення: 01.10.2022).

37. The Ultimate Guide to XDR. URL: https://www.exabeam.com/wp-content/uploads/GUIDE-The-Ultimate-Guide-to-XDR.pdf (дата звернення: 02.10.2022).
38. Jon Oltsik. (2021). Understanding XDR Requirements. URL: https://dbac8a2e962120c65098-4d6abce208e5e17c2085b466b98c2083.ssl.cf1.rackcdn.com/understanding-xdr-requirements-what-xdr-organizations-need-it-pdf-6-w-9311.pdf (дата звернення: 04.10.2022).
39. OPEN XDR VS. NATIVE XDR. (2021). URL: https://www.crowdstrike.com/cybersecurity-101/what-is-xdr/open-xdr-vs-native-xdr/ (дата звернення: 10.10.2022).
40. Open XDR Get Ready to Change Security. URL: https://www.reliaquest.com/solutions/open-xdr/ (дата звернення: 12.10.2022).
41. Gorka Sadowski. (2021). Open XDR versus Native XDR. URL: https://www.exabeam.com/information-security/open-versus-native-xdr/ (дата звернення: 15.10.2022).
42. Stephen Cooper. (2021). 9 Best XDR Tools and Software. URL: https://www.comparitech.com/net-admin/best-xdr-tools/ (дата звернення: 18.10.2022).
43. Блог Тайгер Оптикс.(2021). Cortex XDR: лучшее решение по общему показателю предотвращения и обнаружения угроз в третьем раунде MITRE ATT&CK Evaluations. URL: https://blog.tiger-optics.ru/2021/05/cortex-xdr-mitre-attack-evaluations/ (дата звернення: 21.10.2022).
44. Блиц-огляд проблематики захисту від несанкціонованих дій на прикладах характерних реалізацій / Лєсная Ю. та ін. Problems of the development of modern science. Proceedings of the XXXIV International Scientific and Practical Conference. Madrid, Spain. 2022. Pp. 326-329 URL: https://isg-konf.com/problems-of-the-development-of-modern-science/

45. Погоріла К.В., Богданова Є.С., Колованова Є.П. Огляд можливостей та узагальнення специфіки реалізації XDR-технології, як засобу комплексної протидії актуальним загрозам інформаційної безпеки. Технології, інструменти та стратегії реалізації наукових досліджень: матеріали IV Міжнародної наукової конференції, м. Суми, 7 жовтня, 2022 р. / Міжнародний центр наукових досліджень. — Вінниця: Європейська наукова платформа, 2022. — 142 с.DOI10.36074/mcnd-07.10.2022
46. Всё что вы хотели узнать об XDR в одном посте. (2021). URL: https://habr.com/ru/post/551128/ (дата звернення: 28.10.2022).
47. Отчёт об исследовании утечек информации ограниченного доступа в 2021 году. URL: https://www.infowatch.ru/sites/default/files/analytics/files/v-2021-stalo-bolshe-umyshlennykh-utechek.pdf (дата звернення: 03.11.2022).
48. Концепция обеспечения информационной безопасности предприятия.URL: http://securitypolicy.ru (дата звернення: 03.11.2022).
49. Гліб Веселовський. (2021). Почему Cortex XDR является лучшим решением на рынке? URL: https://expert.com.ua/139678-pochemu-cortex-xdr-yavlyaetsya-luchshim-resheniem-na-rynke.html (дата звернення: 06.11.2022).
50. Compare Cynet 360 vs Cortex XDR. URL: https://expertinsights.com/compare/cynet-360-vs-cortex-xdr (дата звернення: 09.11.2022).
51. Bogdanova, E., Pavlova, L., Pohorila, K. (2022). A concise overview of the specific features of using exployts. Комп'ютерні науки та кібербезпека, (1), 15-19. https://doi.org/10.26565/2519-2310-2022-1-02
52. Мелкозьорова, О., Лєсная, Ю., Малахов, С. (2022). Особливості забезпечення захисту від НСД в сучасних інформаційних системах. *InterConf*, (97). вилучено із: https://ojs.ukrlogos.in.ua/index.php/interconf/article/view/18428
53. Мелкозьорова, О., Лєсная, Ю., Малахов , С. (2022). Особливості інтеграції систем захисту від несанкціонованих дій в сучасних інформаційних системах. Комп'ютерні науки та кібербезпека, (1), 40-45. вилучено із https://periodicals.karazin.ua/cscs/article/view/20912

54. Іваненко, Д., Прищепа, О. (2021). Оцінка ефективності сканерів безпеки веб-додатків. *Комп'ютерні науки та кібербезпека*, (2), 4-14. https://doi.org/10.26565/2519-2310-2021-2-01)
55. Грибунин В.Г. Цифровая стеганография / Грибунин В. Г., Оков И. Н., Туринцев И. В. – М.: Солон-Пресс, 2002. – 272 с
56. Дослідження параметру «серій опорних блоків», як елементу композитного ключа екстрактора даних стеганоалгоритму / Гончаров М. та ін. Problems of science and practice, tasks and ways to solve them. Proceedings of the XX International Scientific and Practical Conference. Warsaw, Poland. 2022. Pp. 779-785 URL: https://isg-konf.com/problems-of-science-and-practice-tasks-and-ways-to-solve-them-two/ Available at: DOI: 10.46299/ISG.2022.1.20
57. Мелкозерова, О., Нарежний, А., Малахов, С. (2021). Верификация отпечатков пальцев посредством декомпозиции минуций и решения задачи коммивояжера. *Збірник наукових праць SCIENTIA*. Вилучено із https://ojs.ukrlogos.in.ua/index.php/scientia/article/view/12415
58. Погоріла К.В., Лєсная Ю.Є., Малахов С.В. (2021). Аналіз структури інсайдерських загроз в іт-сфері та основні складові з протидії цим загрозам. Діджиталізація науки як виклик сьогодення: матеріали II Міжнародної наукової конференції, м. Одеса, 17 грудня, 2021 р. / Міжнародний центр наукових досліджень. — Вінниця: Європейська наукова платформа, 2021. — 123 с. DOI 10.36074/liga-inter-17.12.2021
59. Чорна Т., Богданова Є., Погоріла К. Проблематика доксингу: - міжнародний досвід щодо забезпечення захисту персональних даних // Study of world opinion regarding the development of science. Proceedings of the IX International Scientific and Practical Conference. Prague, Czech Republic. 2022. Pp. 720-723 URL: https://isg-konf.com/study-of-world-opinion-regarding-the-development-of-science/Available at: DOI: 10.46299/ISG.2022.2.9

ДОДАТОК А

PROBLEMS OF THE DEVELOPMENT OF MODERN SCIENCE

Proceedings of the XXXIV International Scientific and Practical Conference

Madrid, Spain
August 30 – September 02, 2022

TECHNICAL SCIENCES
PROBLEMS OF THE DEVELOPMENT OF MODERN SCIENCE

БЛИЦ-ОГЛЯД ПРОБЛЕМАТИКИ ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНИХ ДІЙ НА ПРИКЛАДАХ ХАРАКТЕРНИХ РЕАЛІЗАЦІЙ

Лєсная Юлія Євгенївна
студентка факультету комп'ютерних наук, (бакалавр)
Харківський національний університет імені В.Н. Каразіна, Україна

Погоріла Каріна Валеріївна
студентка факультету комп'ютерних наук, (магістратура)
Харківський національний університет імені В.Н. Каразіна, Україна

Чорна Тетяна Едуардівна
студентка факультету комп'ютерних наук, (бакалавріат)
Харківський національний університет імені В.Н. Каразіна, Україна

Малахов Сергій Віталійович
канд. техн. наук, ст. науковий співробітник, доцент кафедри
Харківський національний університет імені В.Н. Каразіна, Україна

Аналіз досвіду у сфері розробки та модернізації інформаційних систем (ІС), які задіяні при виконанні особливо відповідальних технологічних процедур та/або процесів, дозволяє констатувати, що реалізований у них рівень легітимації виконання критичних циклів управління, визначає фактичний рівень безпеки застосування за призначенням відповідних ІС та/або комплексів автоматизації. Ця ситуація характерна, як при вирішенні завдань управління суто технічними засобами та/або технологічними процесами, так і під час реалізації гібридних схем управління, де в якості безпосередніх об'єктів управління та/або проміжних ланок управління, виступає персонал або великі групи користувачів інформаційних послуг, котрі надаються в рамках діючих інформаційно-комунікаційних платформ та сервісів [1-3].

Забезпечення необхідного рівня легітимації виконання критичних процедур управління, реалізується шляхом комплексної інтеграції до складу базових ІС (*тобто систем що захищаються*), відповідних елементів підсистеми (*або засобів*) захисту від несанкціонованих дій (НСД). При цьому під «легітимацією процедур управління» слід розуміти процес надання необхідного/заданого рівня гарантій стосовно безумовної відповідності реалізованих процедур управління, вимогам технічної, експлуатаційної та нормативної документації базової ІС. Реалізація зазначених гарантій забезпечується шляхом впровадження комплексу спеціальних організаційно-технічних заходів, що передбачають взаємну інтеграцію процесів інформаційної взаємодії базової ІС і підсистеми захисту від НДС при суворому дотриманні встановленого порядку спільних дій персоналу базової ІС, в межах реалізації критичних циклів та/або процедур управління.

326

Рисунок А.1 – Апробація результатів, робота [44], ст. 326

МАТЕРІАЛИ
IV МІЖНАРОДНОЇ
НАУКОВОЇ КОНФЕРЕНЦІЇ

Міжнародний Центр Наукових Досліджень

ТЕХНОЛОГІЇ, ІНСТРУМЕНТИ
ТА СТРАТЕГІЇ РЕАЛІЗАЦІЇ
НАУКОВИХ ДОСЛІДЖЕНЬ

7 ЖОВТНЯ 2022 РІК
м. Суми, Україна

Вінниця, Україна
«Європейська наукова платформа»
2022

7 жовтня 2022 рік ♦ Суми, Україна ♦ МЦНД

ОГЛЯД МОЖЛИВОСТЕЙ ТА УЗАГАЛЬНЕННЯ СПЕЦИФІКИ РЕАЛІЗАЦІЇ XDR-ТЕХНОЛОГІЇ, ЯК ЗАСОБУ КОМПЛЕКСНОЇ ПРОТИДІЇ АКТУАЛЬНИМ ЗАГРОЗАМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Погоріла Каріна Валеріївна
студентка факультету комп'ютерних наук (магістратура)
Харківський національний університет імені В.Н. Каразіна, Україна

Богданова Єлизавета Сергіївна
студентка факультету комп'ютерних наук (бакалаврат)
Харківський національний університет імені В.Н. Каразіна, Україна

Науковий керівник: Колованова Євгенія Павлівна
канд. техн. наук, доцент кафедри безпеки інформаційних систем і технологій
Харківський національний університет імені В.Н. Каразіна, Україна

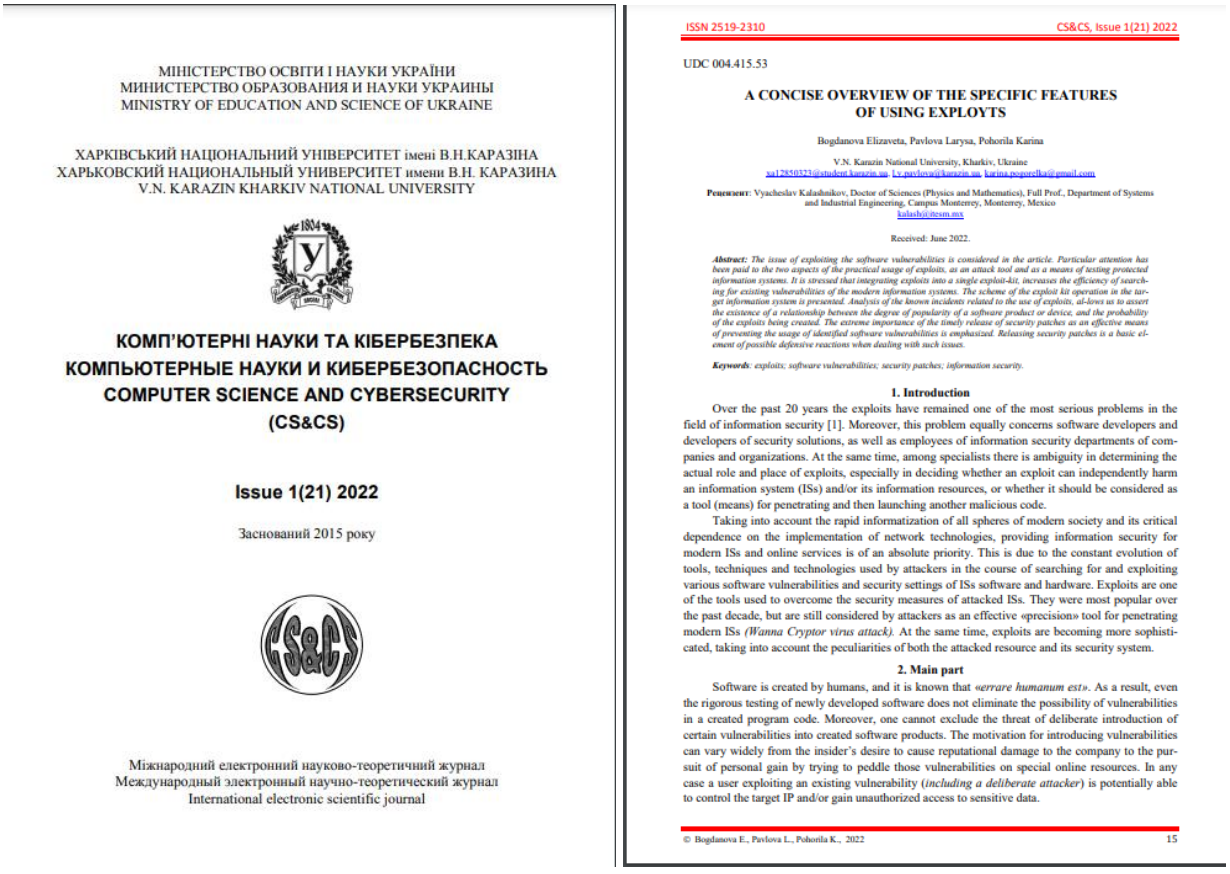
Вступ. На сьогоднішній день далеко не всі організації можуть дозволити собі мати штат фахівців з питань інформаційної безпеки (ІБ) для ефективної експлуатації всіх наявних у них систем та/або інструментів забезпечення ІБ, у рамках єдиного процесу роботи з інцидентами безпеки, оскільки глобальна нестача кваліфікованих профільних кадрів, продовжує залишатися ключовою проблемою на ринку праці. Більш того, велика кількість консолей управління та труднощі з інтеграцією між різними рішеннями ІБ, є причиною неможливості зіставлення подій, що отримані із різних джерел у єдиний інцидент, а також нестачі прозорості в масштабах усього підприємства. Все це веде до «сліпих зон» в контурі безпеки ІБ і супроводжується великою кількістю *«ручних»* завдань, що погіршує показники середнього часу виявлення та реагування на загрози (***MTTD*** - *Mean Time to Detect та* ***MTTR*** - *Mean Time to Repair*).

Основна частина. Зазначений набір труднощів потребує пошуку якогось рішення. Замість того, щоб розширювати наявний корпоративний арсенал розрізненими інструментами і засобами забезпечення ІБ, організаціям пропонується звернути увагу на питання уніфікації їх захисту та підвищення ефективності роботи персоналу, котрий залучається для забезпечення ІБ корпоративних ресурсів. Саме для вирішення подібних труднощів було розроблено клас *XDR* рішень (*Extended Detection and Response*), що входить до трійки найкращих проектів у галузі кібербезпеки у 2021 році [4].

В цілому, XDR це платформа моніторингу ІБ, що забезпечує багатофакторний контроль та автоматичне реагування на інциденти не тільки на кінцевих точках, але і на набагато інших елементах корпоративної інфраструктури: від мобільних телефонів співробітників до хмарних додатків. Процес роботи зі складними інцидентами ІБ, що пов'язані з інтегральними загрозами безпеки та таргетованими атаками по цільовим елементами корпоративної інфраструктури [5], передбачає наявність автоматизованого процесу реагування, а точніше - виконання швидких і точних дій зі збирання потрібних відомостей, виявлення атипових мережевих ознак, аудиту телеметрії ІБ, та парирування відповідних загроз. Саме на цьому і сфокусовані зусилля розробників *XDR* платформ.

Важливо підкреслити, що технології *розширеного* виявлення та реагування мають ряд суттєвих переваг перед технологією розширеного виявлення і реагування

Рисунок А.2 – Апробація результатів, робота [45], ст. 61



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ
MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені В.Н.КАРАЗІНА
ХАРЬКОВСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ имени В.Н. КАРАЗИНА
V.N. KARAZIN KHARKIV NATIONAL UNIVERSITY

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА
КОМПЬЮТЕРНЫЕ НАУКИ И КИБЕРБЕЗОПАСНОСТЬ
COMPUTER SCIENCE AND CYBERSECURITY
(CS&CS)

Issue 1(21) 2022

Заснований 2015 року

Міжнародний електронний науково-теоретичний журнал
Международный электронный научно-теоретический журнал
International electronic scientific journal

ISSN 2519-2310 CS&CS, Issue 1(21) 2022

UDC 004.415.53

A CONCISE OVERVIEW OF THE SPECIFIC FEATURES OF USING EXPLOYTS

Bogdanova Elizaveta, Pavlova Larysa, Pohorila Karina

V.N. Karazin National University, Kharkiv, Ukraine
sa12850323@student.karazin.ua, l.v.pavlova@karazin.ua, karina.pogorelka@gmail.com

Рецензент: Vyacheslav Kalashnikov, Doctor of Sciences (Physics and Mathematics), Full Prof., Department of Systems and Industrial Engineering, Campus Monterrey, Monterrey, Mexico
kalash@itesm.mx

Received: June 2022.

Abstract: *The issue of exploiting the software vulnerabilities is considered in the article. Particular attention has been paid to the two aspects of the practical usage of exploits, as an attack tool and as a means of testing protected information systems. It is stressed that integrating exploits into a single exploit-kit, increases the efficiency of searching for existing vulnerabilities of the modern information systems. The scheme of the exploit kit operation in the target information system is presented. Analysis of the known incidents related to the use of exploits, al-lows us to assert the existence of a relationship between the degree of popularity of a software product or device, and the probability of the exploits being created. The extreme importance of the timely release of security patches as an effective means of preventing the usage of identified software vulnerabilities is emphasized. Releasing security patches is a basic element of possible defensive reactions when dealing with such issues.*

Keywords*: exploits; software vulnerabilities; security patches; information security.*

1. Introduction

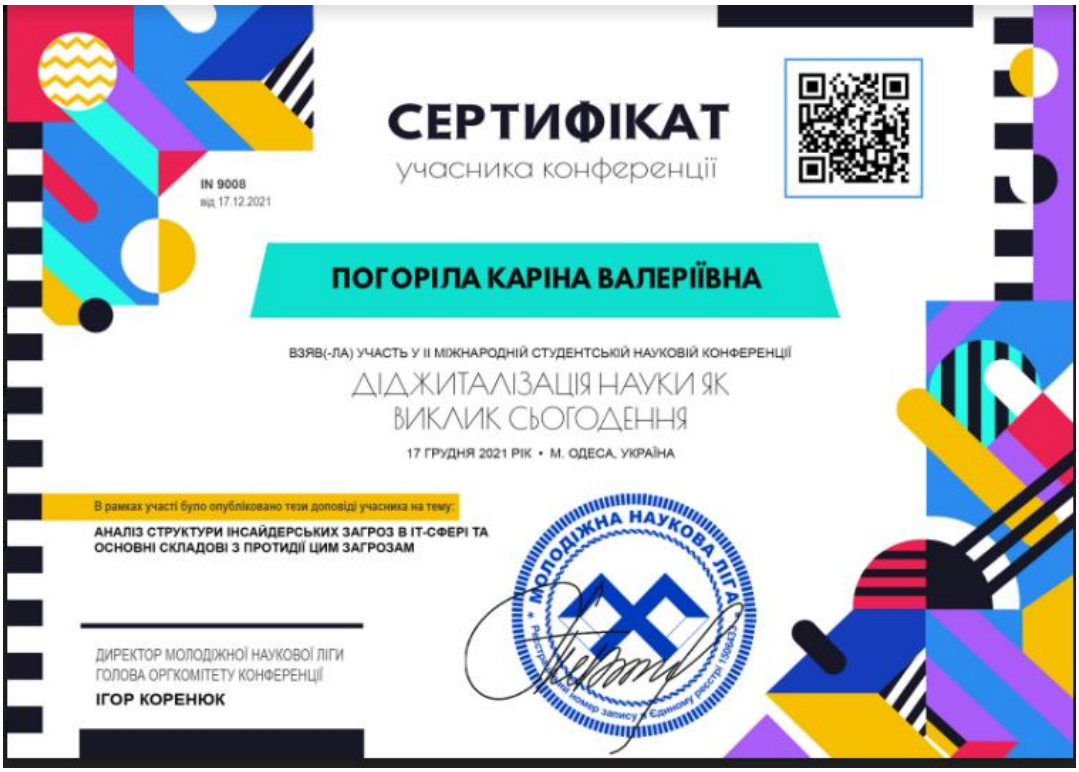
Over the past 20 years the exploits have remained one of the most serious problems in the field of information security [1]. Moreover, this problem equally concerns software developers and developers of security solutions, as well as employees of information security departments of companies and organizations. At the same time, among specialists there is ambiguity in determining the actual role and place of exploits, especially in deciding whether an exploit can independently harm an information system (ISs) and/or its information resources, or whether it should be considered as a tool (means) for penetrating and then launching another malicious code.

Taking into account the rapid informatization of all spheres of modern society and its critical dependence on the implementation of network technologies, providing information security for modern ISs and online services is of an absolute priority. This is due to the constant evolution of tools, techniques and technologies used by attackers in the course of searching for and exploiting various software vulnerabilities and security settings of ISs software and hardware. Exploits are one of the tools used to overcome the security measures of attacked ISs. They were most popular over the past decade, but are still considered by attackers as an effective «precision» tool for penetrating modern ISs *(Wanna Cryptor virus attack)*. At the same time, exploits are becoming more sophisticated, taking into account the peculiarities of both the attacked resource and its security system.

2. Main part

Software is created by humans, and it is known that *«errare humanum est»*. As a result, even the rigorous testing of newly developed software does not eliminate the possibility of vulnerabilities in a created program code. Moreover, one cannot exclude the threat of deliberate introduction of certain vulnerabilities into created software products. The motivation for introducing vulnerabilities can vary widely from the insider's desire to cause reputational damage to the company to the pursuit of personal gain by trying to peddle those vulnerabilities on special online resources. In any case a user exploiting an existing vulnerability (*including a deliberate attacker*) is potentially able to control the target IP and/or gain unauthorized access to sensitive data.

Рисунок А.3 – Апробація результатів, робота [51], ст. 15



СЕРТИФІКАТ

учасника конференції

IN 9008
від 17.12.2021

ПОГОРІЛА КАРІНА ВАЛЕРІЇВНА

ВЗЯВ(-ЛА) УЧАСТЬ У II МІЖНАРОДНІЙ СТУДЕНТСЬКІЙ НАУКОВІЙ КОНФЕРЕНЦІЇ

ДІДЖИТАЛІЗАЦІЯ НАУКИ ЯК ВИКЛИК СЬОГОДЕННЯ

17 ГРУДНЯ 2021 РІК • М. ОДЕСА, УКРАЇНА

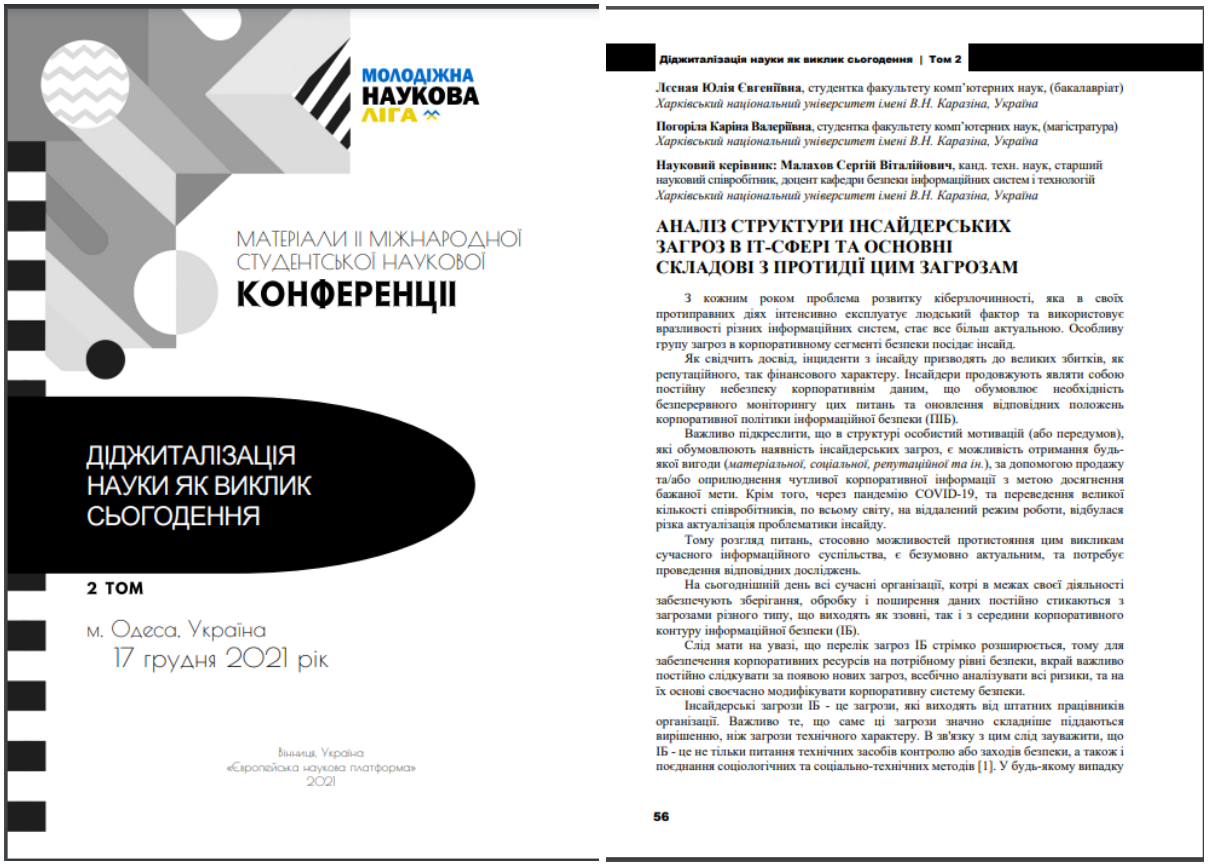
В рамках участі було опубліковано тези доповіді учасника на тему:

АНАЛІЗ СТРУКТУРИ ІНСАЙДЕРСЬКИХ ЗАГРОЗ В ІТ-СФЕРІ ТА ОСНОВНІ СКЛАДОВІ З ПРОТИДІЇ ЦИМ ЗАГРОЗАМ

МОЛОДІЖНА НАУКОВА ЛІГА

ДИРЕКТОР МОЛОДІЖНОЇ НАУКОВОЇ ЛІГИ
ГОЛОВА ОРГКОМІТЕТУ КОНФЕРЕНЦІЇ
ІГОР КОРЕНЮК

Рисунок А.4 – Апробація результатів, робота [58]



МОЛОДІЖНА НАУКОВА ЛІГА

МАТЕРІАЛИ II МІЖНАРОДНОЇ СТУДЕНТСЬКОЇ НАУКОВОЇ КОНФЕРЕНЦІЇ

ДІДЖИТАЛІЗАЦІЯ НАУКИ ЯК ВИКЛИК СЬОГОДЕННЯ

2 ТОМ

м. Одеса, Україна
17 грудня 2021 рік

Віденець, Україна
«Європейська наукова платформа»
2021

Діджиталізація науки як виклик сьогодення | Том 2

Лєсная Юлія Євгенівна, студентка факультету комп'ютерних наук, (бакалавріат)
Харківський національний університет імені В.Н. Каразіна, Україна

Погоріла Каріна Валеріївна, студентка факультету комп'ютерних наук, (магістратура)
Харківський національний університет імені В.Н. Каразіна, Україна

Науковий керівник: Малахов Сергій Віталійович, канд. техн. наук, старший науковий співробітник, доцент кафедри безпеки інформаційних систем і технологій
Харківський національний університет імені В.Н. Каразіна, Україна

АНАЛІЗ СТРУКТУРИ ІНСАЙДЕРСЬКИХ ЗАГРОЗ В ІТ-СФЕРІ ТА ОСНОВНІ СКЛАДОВІ З ПРОТИДІЇ ЦИМ ЗАГРОЗАМ

З кожним роком проблема розвитку кіберзлочинності, яка в своїх протиправних діях інтенсивно експлуатує людський фактор та використовує вразливості різних інформаційних систем, стає все більш актуальною. Особливу групу загроз в корпоративному сегменті безпеки посідає інсайд.

Як свідчить досвід, інциденти з інсайду призводять до великих збитків, як репутаційного, так фінансового характеру. Інсайдери продовжують являти собою постійну небезпеку корпоративним даним, що обумовлює необхідність безперервного моніторингу цих питань та оновлення відповідних положень корпоративної політики інформаційної безпеки (ПІБ).

Важливо підкреслити, що в структурі особистий мотивацій (або передумов), які обумовлюють наявність інсайдерських загроз, є можливість отримання будь-якої вигоди (*матеріальної, соціальної, репутаційної та ін.*), за допомогою продажу та/або оприлюднення чутливої корпоративної інформації з метою досягнення бажаної мети. Крім того, через пандемію COVID-19, та переведення великої кількості співробітників, по всьому світу, на віддалений режим роботи, відбулася різка актуалізація проблематики інсайду.

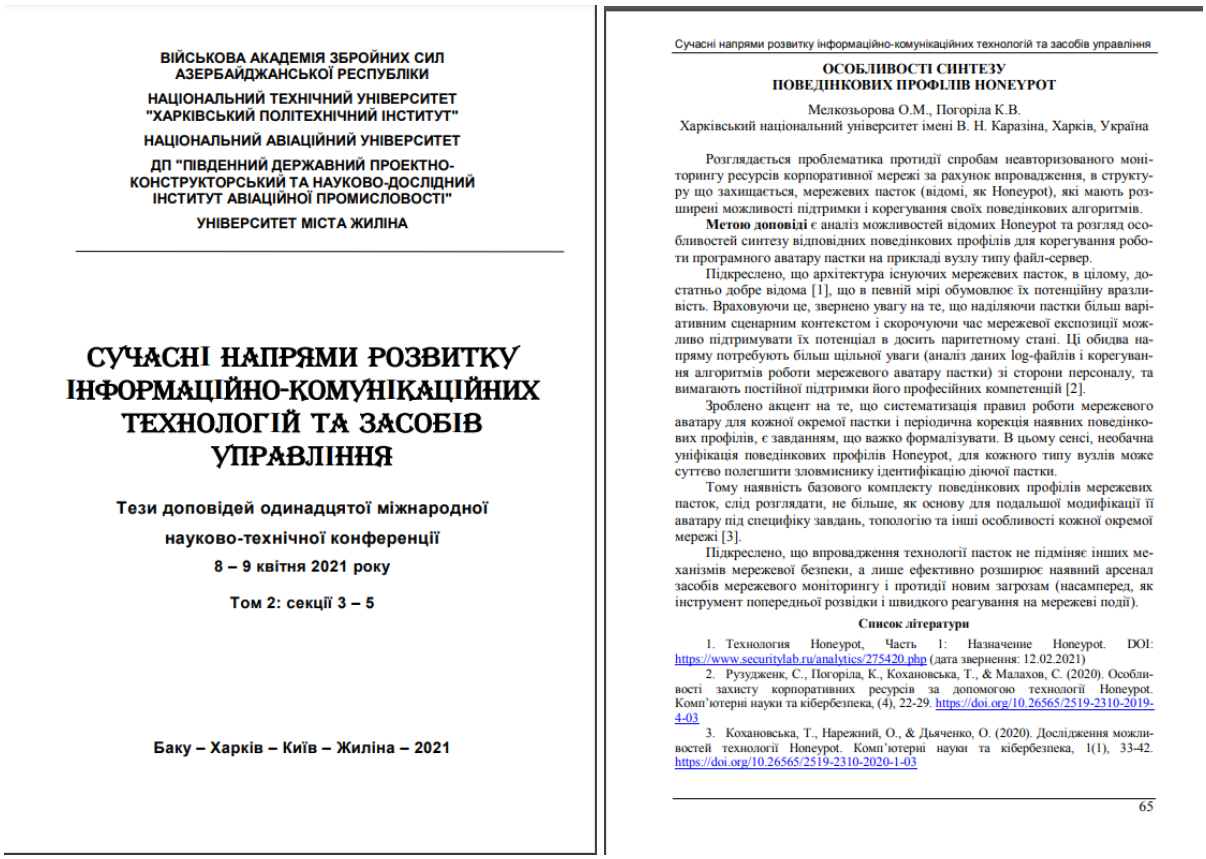
Тому розгляд питань, стосовно можливостей протистояння цим викликам сучасного інформаційного суспільства, є безумовно актуальним, та потребує проведення відповідних досліджень.

На сьогоднішній день всі сучасні організації, котрі в межах своєї діяльності забезпечують зберігання, обробку і поширення даних постійно стикаються з загрозами різного типу, що виходять як ззовні, так і з середини корпоративного контуру інформаційної безпеки (ІБ).

Слід мати на увазі, що перелік загроз ІБ стрімко розширюється, тому для забезпечення корпоративних ресурсів на потрібному рівні безпеки, вкрай важливо постійно слідкувати за появою нових загроз, всебічно аналізувати всі ризики, та на їх основі своєчасно модифікувати корпоративну систему безпеки.

Інсайдерські загрози ІБ - це загрози, які виходять від штатних працівників організації. Важливо те, що саме ці загрози значно складніше піддаються вирішенню, ніж загрози технічного характеру. В зв'язку з цим слід зауважити, що ІБ - це не тільки питання технічних засобів контролю або заходів безпеки, а також і поєднання соціологічних та соціально-технічних методів [1]. У будь-якому випадку

Рисунок А.5 – Апробація результатів, робота [58], ст. 56



ВІЙСЬКОВА АКАДЕМІЯ ЗБРОЙНИХ СИЛ АЗЕРБАЙДЖАНСЬКОЇ РЕСПУБЛІКИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ "ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ДП "ПІВДЕННИЙ ДЕРЖАВНИЙ ПРОЕКТНО-КОНСТРУКТОРСЬКИЙ ТА НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ АВІАЦІЙНОЇ ПРОМИСЛОВОСТІ"

УНІВЕРСИТЕТ МІСТА ЖИЛІНА

СУЧАСНІ НАПРЯМИ РОЗВИТКУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЗАСОБІВ УПРАВЛІННЯ

Тези доповідей одинадцятої міжнародної науково-технічної конференції

8 – 9 квітня 2021 року

Том 2: секції 3 – 5

Баку – Харків – Київ – Жиліна – 2021

Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління

ОСОБЛИВОСТІ СИНТЕЗУ ПОВЕДІНКОВИХ ПРОФІЛІВ HONEYPOT

Мелкозьорова О.М., Погоріла К.В.
Харківський національний університет імені В. Н. Каразіна, Харків, Україна

Розглядається проблематика протидії спробам неавторизованого моніторингу ресурсів корпоративної мережі за рахунок впровадження, в структуру що захищається, мережевих пасток (відомі, як Honeypot), які мають розширені можливості підтримки і корегування своїх поведінкових алгоритмів.

Метою доповіді є аналіз можливостей відомих Honeypot та розгляд особливостей синтезу відповідних поведінкових профілів для корегування роботи програмного аватару пастки на прикладі вузлу типу файл-сервер.

Підкреслено, що архітектура існуючих мережевих пасток, в цілому, достатньо добре відома [1], що в певній мірі обумовлює їх потенційну вразливість. Враховуючи це, звернено увагу на те, що наділяючи пастки більш варіативним сценарним контекстом і скорочуючи час мережевої експозиції можливо підтримувати їх потенціал в досить паритетному стані. Ці обидва напряму потребують більш щільної уваги (аналіз даних log-файлів і корегування алгоритмів роботи мережевого аватару пастки) зі сторони персоналу, та вимагають постійної підтримки його професійних компетенцій [2].

Зроблено акцент на те, що систематизація правил роботи мережевого аватару для кожної окремої пастки і періодична корекція наявних поведінкових профілів, є завданням, що важко формалізувати. В цьому сенсі, необачна уніфікація поведінкових профілів Honeypot, для кожного типу вузлів може суттєво полегшити зловмиснику ідентифікацію діючої пастки.

Тому наявність базового комплекту поведінкових профілів мережевих пасток, слід розглядати, не більше, як основу для подальшої модифікації її аватару під специфіку завдань, топологію та інші особливості кожної окремої мережі [3].

Підкреслено, що впровадження технології пасток не підміняє інших механізмів мережевої безпеки, а лише ефективно розширює наявний арсенал засобів мережевого моніторингу і протидії новим загрозам (насамперед, як інструмент попередньої розвідки і швидкого реагування на мережеві події).

Список літератури

1. Технология Honeypot, Часть 1: Назначение Honeypot. DOI: https://www.securitylab.ru/analytics/275420.php (дата звернення: 12.02.2021)
2. Рузунженк, С., Погоріла, К., Кохановська, Т., & Малахов, С. (2020). Особливості захисту корпоративних ресурсів за допомогою технології Honeypot. Комп'ютерні науки та кібербезпека, (4), 22-29. https://doi.org/10.26565/2519-2310-2019-4-03
3. Кохановська, Т., Нарежний, О., & Дьяченко, О. (2020). Дослідження можливостей технології Honeypot. Комп'ютерні науки та кібербезпека, 1(1), 33-42. https://doi.org/10.26565/2519-2310-2020-1-03

65

Рисунок А.6 – Апробація результатів, робота [21], ст. 65

ISSN 2519-2310

CS&CS Journal

KARAZIN UNIVERSITY
CLASSICS AHEAD OF TIME

4(16) 2019

COMPUTER SCIENCE AND CYBERSECURITY

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА

ISSN 2519-2310 CS&CS, Issue 4(16) 2019

УДК 004.056.5 DOI: 10.26565/2519-2310-2019-4-03

ОСОБЛИВОСТІ ЗАХИСТУ КОРПОРАТИВНИХ РЕСУРСІВ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЇ HONEYPOT

Сабіна Рузунженк, Карина Погоріла, Тетяна Кохановська, Сергій Малахов

Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, Харків, 61022, Україна
ruzudzhenk.jb@gmail.com, karina.pogorelka@gmail.com, tanya.koh09@gmail.com, mailgate@meta.ua

Рецензент: Олександр Оксіюк, д.т.н., проф., Київський національний університет імені Т. Шевченка, вул. М. Ломоносова 81, Київ, 03189, Україна.
o.oksiuk@gmail.com

Поступила: Листопад 2019.

Анотація: У статті надано стислий огляд основних можливостей технології Honeypot. Розглянуті питання стосовно: - особливостей моніторингу мережевої активності на різних етапах розвитку атак/вторгнень; - розміщення датчиків системи; - процедур збору та узагальнення даних щодо мережевих подій; - варіантів модифікації інструментів захисту; - організації структури захисту тощо. Розглянуті загальні принципи роботи відповідних систем на базі відокремлених серверів та програмно емульованих мереж. Узагальнено основні недоліки даної технології. Звернено увагу на перспективність використання різноманітних рішень Honeypot для цілей розширення потенціалу вже розгорнутих засобів забезпечення інформаційної безпеки (ІБ).

Ключові слова: Honeypot; вторгнення; інформаційна безпека; ЛОМ; Firewall; IDS; IPS.

1 Вступ

У сучасному світі інформаційних технологій кожен Інтернет користувач та локальна обчислювальна мережа, які мають підключення до Інтернет, рано чи пізно, але в будь-якому випадку, неминуче стикаються з проблемою зовнішніх кібератак. Враховуючи цей факт, як аксіому, можна зробити висновок, що відповідні інформаційні і апаратні ресурси Інтернет користувачів та локальних обчислювальних мереж (ЛОМ), що взаємодіють з Інтернет, обов'язково повинні бути спроможні парирувати відповідні загрози. Саме тому, на постійній основі, необхідно забезпечувати комплексний моніторинг поточної мережевої активності, особливо в частині аналізу змісту, характеру та інтенсивності трансграничного трафіку. В першу чергу це стосується аналізу трафіку в межах спеціально передбачених демілітаризованих зон, або відповідних публічних сервісів (*при їх наявності*), що передбачають інтенсивну взаємодію з користувачами, які знаходяться за рамками організованого периметра безпеки компанії або окремого користувача. Одним з ефективних засобів ведення моніторингу мережевої активності та виявлення ознак підготовки майбутнього кіберзлочини, є використання можливостей технології Honeypot (*т.з. вузлів або мереж пасток/приманок*). Крім того потенціал Honeypot дозволяє, в буквальному сенсі, виграти час, відволікаючи мережевого зловмисника або спеціалізовану програму на виконання завідомо зайвих або хибних дій.

Аналіз джерел. Honeypot вперше з'явилися з першими комп'ютерними зловмисниками, а практика їх активного використання налічує вже більше 20 років. Роботи по їх створенню та практичному впровадженню проводилися паралельно з дослідженнями IDS та IPS [1]. Першою документальною згадкою за тематикою Honeypot, була робота Кліффорда Столла «The Cuckoo's Egg», що вийшла у 1990 році. А вже у 2000-х роках Honeypot стали досить поширеними системами, що забезпечували ефективну протидію спробам несанкціонованого проникнення до «внутрішнього» периметру безпеки комп'ютерних мереж компаній.

На сьогоднішній день актуальним напрямом використання вузлів і мереж – приманок є, наприклад, протистояння дням кіберзлочинців при парируванні розгалужених атак типу «відмова в обслуговуванні (*DDos*) при використанні різних моделей хмарних обчислень (*наприклад, PAAS або IAAS*). Застосування Honeypot полегшує збір інформації про потенційну атаку і атакуючого вже на етапах підготовки (*попередньої розвідки*) та початку «проникнення» в

 22

Рисунок А.7 – Апробація результатів, робота [22], ст. 22

CERTIFICATE

Google Scholar
Bowker
INTERNATIONAL SCIENCE GROUP
OUCI
Open Ukrainian Citation Index
Crossref
Content Registration

is awarded to

Погоріла Каріна Валеріївна

for active participation
IX International Scientific and Practical Conference
«STUDY OF WORLD OPINION REGARDING THE DEVELOPMENT OF SCIENCE»

November 22 – 25, 2022, Prague, Czech Republic
24 Hours of Participation
(0,8 ECTS credits)

Organizing committee Ekaterina Zvereva

Рисунок А.8 – Апробація результатів, робота [59]

International Science Group
ISG-KONF.COM

IX
INTERNATIONAL SCIENTIFIC
AND PRACTICAL CONFERENCE
"STUDY OF WORLD OPINION REGARDING THE
DEVELOPMENT OF SCIENCE"

Prague, Czech Republic
November 22 - 25, 2022

ISBN 979-8-88831-927-7
DOI 10.46299/ISG.2022.2.9

TECHNICAL SCIENCES
STUDY OF WORLD OPINION REGARDING THE DEVELOPMENT OF SCIENCE

ПРОБЛЕМАТИКА ДОКСИНГУ: - МІЖНАРОДНИЙ ДОСВІД ЩОДО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Чорна Тетяна Едуардівна
студентка факультету комп'ютерних наук, (бакалавріат)
Харківський національний університет імені В.Н. Каразіна, Україна

Богданова Єлизавета Сергіївна
студентка факультету комп'ютерних наук, (бакалавріат)
Харківський національний університет імені В.Н. Каразіна, Україна

Погоріла Каріна Валеріївна
студентка факультету комп'ютерних наук, (магістрат)
Харківський національний університет імені В.Н. Каразіна, Україна

В сучасному суспільстві, проблематика доксингу є однією з найбільш обговорюваних тем. Це відносно нове явище, що є похідною формування парадигми існування сучасного інформаційного суспільства. Актуальність цього напряму, спонукає профільних фахівців проводити ретельний аналіз відповідних інцидентів, з метою завчасного усунення передумов виникнення подібних загроз у майбутньому. Так наприклад, учасниками дослідження Нью-Йоркського університету 2017 року було виявлено та проаналізовано понад 5500 файлів, що були пов'язані із доксуванням [1]. Їх результати свідчать, що понад 90% доксованих файлів містили адресу жертви, 61% - номер телефону, а 53% - адресу електронної пошти жертв атаки. Більш того, сорок відсотків імен онлайн користувачів були оприлюднені, і такий же самий відсоток IP-адрес жертв атаки, було викладено в загальний доступ. Менш поширена, персоніфікована інформація, така як, номери кредитних карток (4,3%), номери соціального страхування (2,6%) або інша фінансова інформація (8,8%), також була розкрита (див. рис. 1).

Здійснюючи спробу захистити особисту інформацію, яка розміщена в соціальних мережах: - 32% жертв доксингу «закрили» або змінили особисті налаштування конфіденційності у своєму обліковому записі Instagram, а 25% змінили поточні налаштування облікового запису Facebook (після атаки). Приблизно 10% жертв цієї атаки змінили свій обліковий запис у Instagram, а 3% змінили свої налаштування у Facebook, після того, як було вжито заходів щодо боротьби зі зловживаннями.

Розглядаючи питання захисту конфіденційної інформації з юридичного боку, розкривається вся складність цієї проблеми. Зазвичай, в таких випадках, можна говорити про порушення законодавства про персональні дані, але коли йдеться про наслідки інциденту, важко притягти до відповідальності конкретну людину (виконавця та/або замовника атаки). Проте з метою запобігання, а також

720

Рисунок А.9 — Апробація результатів на МНПК [59], сторінка 720