Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«__» _____ 2025 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

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

спеціальність *125 Кібербезпека та захист інформації*
(код і назва спеціальності)

освітній ступень *магістр*

освітньо-наукова програма *Кібербезпека*
(назва освітньої програми)

на тему: «Метод тестування систем захисту з використанням симуляції кібератак»

Виконавець: студент ІІ курсу, групи КБм-21

_____ **Ярослав СІЧКАР**
(підпис) (Ім'я, ПРІЗВИЩЕ)

	Ім'я, ПРІЗВИЩЕ	**Підпис**
Науковий керівник	Леся БАРАНОВСЬКА	
Нормоконтроль	Юрій БАБЕНКО	

Київ 2025

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«25» жовтня 2024 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності *125 Кібербезпека та захист інформації*
(код і назва спеціальності)

освітній ступень *магістр*

Здобувача(ки) КБм-21 (група) Січкаря Ярослава Сергійовича (прізвище ім'я по-батькові)

Тема кваліфікаційної роботи Метод тестування систем захисту з використанням симуляції кібератак.

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 4 від 24.10.2024 р.

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень	процес тестування систем захисту.
Предмет досліджень	процедури та механізми тестування систем захисту з використанням автоматизованої симуляції кібератак.
Мета	розробка методу тестування систем захисту з використанням автоматизованої симуляції кібератак.
Вихідні дані для проведення роботи	Сучасне законодавство України в сфері кібербезпеки, актуальні системи симуляції кібератак.

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна Вперше розроблено метод тестування систем захисту з використанням автоматизованої симуляції кібератак.

Практична цінність Використання створеного методу для тестування систем захисту за допомогою симуляцій кібератак.

4. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Уточнення постановки задачі	25.10.2024 – 15.11.2024
Аналіз літературних джерел	16.11.2024 – 04.01.2025
Аналіз сучасних підходів до тестування систем захисту, їх переваг та недоліків	05.01.2025 – 06.02.2025
Аналіз сучасних систем симуляції кібератак	07.02.2025 – 02.03.2025
Розробка методу тестування систем захисту	03.03.2025 – 26.03.2025
Практична перевірка методу	27.03.2025 – 21.04.2025
Оформлення пояснювальної записки згідно методичних рекомендацій	22.04.2025 – 15.05.2025
Подача пакету документів на розгляд ЕК	15.05.2025 – 19.05.2025

Завдання видала _____ Леся БАРАНОВСЬКА
(підпис) (Ім'я, ПРІЗВИЩЕ)

Завдання прийняв до виконання _____ Ярослав СІЧКАР
(підпис) (Ім'я, ПРІЗВИЩЕ)

Дата видачі завдання: 25.10.2024 р.
Термін подання кваліфікаційної роботи до ЕК 19.05.2025 р

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи «Метод тестування систем захисту з використанням симуляції кібератак»: 95 сторінок, 41 рисунок та 2 таблиці, 84 літературних джерела.

Об’єкт дослідження – процес тестування систем захисту.

Мета роботи – розробка методу тестування систем захисту з використанням автоматизованої симуляції кібератак.

Предмет дослідження – процедури та механізми тестування систем захисту з використанням автоматизованої симуляції кібератак.

Методи дослідження – аналіз, порівняння, синтез, експеримент.

Практична цінність – використання створеного методу для тестування систем захисту за допомогою автоматизованої симуляції кібератак.

Актуальність – кількість систем захисту постійно зростає, оскільки спеціалісти з безпеки намагаються не відставати від зловмисників. У зв’язку з цим актуальним стає впровадження ефективних методів щоденного тестування систем захисту для виявлення потенційних прогалин в безпеці до того, як ними скористаються зловмисники. Оскільки пентест або тестування червоної команди (red team) не можуть виконуватись щоденно, одним із перспективних підходів є використання систем симуляції кібератак.

Наукова новизна вперше розроблено метод тестування систем захисту з використанням автоматизованої симуляції кібератак.

Ключові слова: BAS, системи захисту, SIEM, EDR, симуляції кібератак, пентест, red teaming, тестування систем захисту.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

СК	- Симуляція кібератак
СЗ	- Системи захисту
BAS	- Breach and attack simulation
ТС	- Тестування систем
SIEM	- Security Information and Event Management
EDR	- Endpoint Detection and Response
SOAR	- Security orchestration, automation, and response
IPS	- Intrusion Prevention System
IDS	- Intrusion Detection System

ЗМІСТ

ВСТУП

Актуальність. У сучасному цифровому світі кіберзагрози постійно еволюціонують, стаючи дедалі складнішими та спричиняючи все більше збитків. Захист інформаційних систем є критично важливим завданням для організацій різного рівня, адже витоки даних, злам систем або зупинка їх роботи можуть призвести до значних фінансових втрат і репутаційних ризиків.

При цьому кількість систем захисту також постійно зростає, оскільки спеціалісти з безпеки намагаються не відставати від зловмисників. У зв’язку з цим актуальним стає впровадження ефективних методів тестування систем захисту для виявлення потенційних прогалин в безпеці до того, як ними скористаються зловмисники.

Одним із перспективних підходів є використання симуляції кібератак, що дозволяє моделювати реальні загрози і оцінювати здатність системи протидіяти їм у контрольованих умовах. Такий метод забезпечує глибоке розуміння слабких місць захисту та дозволяє розробляти заходи щодо їхнього усунення.

Дослідження методів тестування систем захисту із застосуванням симуляції кібератак сприяє підвищенню рівня кібербезпеки, оскільки дозволяє не лише одноразово оцінити поточний стан захисту, але й регулярно тестувати наявні системи та вдосконалювати механізми виявлення та реагування на загрози.

Метою є розробка методу тестування систем захисту з використанням автоматизованої симуляції кібератак.

Мета обумовлена вирішенням наступних задач:

- Здійснити порівняльний аналіз систем симуляції кібератак з традиційними методами тестування систем захисту.
- Розглянути системи симуляції кібератак, як вони допомагають виявити недоліки в системах захисту та переваги інтеграції таких систем із системами кібербезпеки.

• Розробити метод тестування систем захисту з використанням автоматизованої симуляції кібератак.

• Провести тестування систем захисту за допомогою симуляції кібератак.

Об’єктом дослідження є процес тестування систем захисту, оскільки без чітко побудованого процесу тестування неможливо бути певним у коректності налаштування усіх систем захисту, а також в їх правильній взаємодії.

Предметом дослідження є процедури та механізми тестування систем захисту з використанням автоматизованої симуляції кібератак. Зміни в системи захисту можуть вноситись щоденно, а також щоденно можуть з’являтись нові загрози. Таким чином, важливо автоматизувати процес перевірки систем захисту, щоб це відбувалось на регулярній основі, а адміністратори з безпеки могли в будь-який момент переконатись, що всі системи готові до протидії реальним загрозам.

Практичною цінністю роботи є можливість використання створеного методу для тестування систем захисту за допомогою автоматизованої симуляції кібератак. На даний момент, відсутні регуляторні вимоги які вимагають щоденного тестування систем захисту, відповідно й рекомендації щодо побудови такого тестування також відсутні. Самостійно розробити даний підхід може бути складно для організацій, а отже доцільно буде використати розроблений метод.

Науковою новизною даної роботи є вперше розроблений метод перевірки систем захисту з використанням автоматизованої симуляції кібератак, який організації будь-якого рівня можуть використати для покращення та перевірки кіберзахисту.

Апробація роботи – основні результати роботи публікувались та обговорювались на таких наукових конференціях:

- Січкар Я., Барановська Л. Тестування систем захисту з використанням симуляції кібератак. VIII Міжнародна науково-практична конференція Проблеми кібербезпеки інформаційно-комунікаційних систем” (PCSITS), 11 квітня 2025, Київ, Україна, С. 93-94.

РОЗДІЛ 1
ОБҐРУНТУВАННЯ НЕОБХІДНОСТІ ВПРОВАДЖЕННЯ СУЧАСНИХ ПІДХОДІВ ДО ТЕСТУВАННЯ СИСТЕМ ЗАХИСТУ

1.1 Актуальність перевірки захищеності інформаційних систем

Сучасний світ все більше залежить від цифрових технологій, що робить питання кібербезпеки критично важливим для державних установ, бізнесу та звичайних користувачів. За останні роки кількість кібератак суттєво зросла, а зловмисники використовують все більш витончені методи для досягнення своїх цілей.

Особливо вразливими є компанії малого та середнього бізнесу, які часто не мають достатніх ресурсів для ефективного кіберзахисту. 48% таких компаній зазнали кібератак за 2023 рік [1].

Кіберзлочини завдають серйозної шкоди економіці. За оцінками Statista, глобальні фінансові втрати від кібератак можуть досягти 13.82 трильйона доларів до 2028 року [2]. Це включає прямі втрати від шахрайства, втрату даних, зупинку бізнес-процесів, витрати на юридичні процеси та репутаційні збитки.

Згідно з п'ятим щорічним звітом Sophos "The State of Ransomware 2024", 59% організацій зазнали атак програм-вимагачів у минулому році, що є незначним зниженням порівняно з 66% у попередні два роки [3]. Це свідчить про те, що понад половина організацій все ще стикається з цими загрозами, підкреслюючи необхідність постійного вдосконалення заходів кібербезпеки.

Аналіз за галузями показав, що центральні або федеральні урядові установи зазнали найвищого рівня атак (68%), тоді як державні чи місцеві урядові організації повідомили про значно нижчий показник (34%). Ця різниця може бути пов'язана з різними факторами, включаючи політичні мотиви атак [3].

Нині спостерігається стабільне зростання кількості кібератак, особливо спрямованих на критично важливу інфраструктуру України. Противник продовжує

використовувати кіберзброю для дестабілізації країни, що підтверджує, що кіберпростір залишається одним із ключових фронтів сучасної війни.

Україна залишається однією з основних цілей кіберзлочинців та державних хакерських угруповань. За даними CERT-UA, у 2023 році було зафіксовано 4 315 кіберінцидентів [4]. Це на 69,8% більше, ніж роком раніше, коли кіберзлочинці атакували український кіберпростір 2541 раз.

Зловмисники найчастіше націлюються на місцеві органи влади, урядові установи, структури безпеки та оборони, енергетичний сектор, комерційні компанії та телекомунікаційну галузь. Серед основних видів атак переважають поширення шкідливого програмного забезпечення, фішингові атаки, несанкціоновані підключення, компрометація облікових записів і систем. Головними цілями кіберзлочинців є викрадення конфіденційної інформації, а також знищення даних та інформаційних систем, наприклад як це було під час атаки на оператора мобільного зв'язку Київстар. Під час атаки було знищено більше тисячі віртуальних серверів та персональних комп'ютерів, що свідчить про катастрофічні руйнування [5].

1.2 Розвиток технологій кіберзлочинців

Кіберзлочинці суттєво покращили свої тактики та стратегії за останні роки, що обумовлено досягненнями в галузі технологій, глобалізацією та зростанням залежності від цифрових систем. Розглянемо основні напрямки в яких кіберзлочинці досягли найбільших успіхів.

1.2.1 Використання штучного інтелекту та машинного навчання в кіберзагрозах

Завдяки AI і ML зловмисники можуть швидше знаходити вразливості в системах, аналізувати величезні обсяги даних та автоматично підбирати способи злому. Це дозволяє їм здійснювати атаки з меншою витратою ресурсів та без необхідності ручного налаштування усіх засобів [6].

Одним із ключових напрямів використання AI є створення високоякісних фішингових атак. Генеративний штучний інтелект (наприклад, моделі GPT) дає змогу автоматично генерувати правдоподібні електронні листи, які імітують стиль офіційного спілкування. Завдяки цьому потенційні жертви частіше відкривають фішингові повідомлення та вводять свої облікові дані на шахрайських сайтах [7].

Машинне навчання використовується для створення шкідливого ПЗ, яке може змінювати свою поведінку в реальному часі, щоб уникати виявлення антивірусними програмами. Таке ПЗ аналізує середовище, в якому працює, і коригує свою тактику залежно від умов, що значно ускладнює його нейтралізацію.

Окремий виклик становить використання генеративного штучного інтелекту для створення правдоподібних аудіо та відео [8]. Наприклад, deepfake-технології дозволяють підробляти голоси або обличчя людей, що підвищує ризики шахрайства та кібершпигунства. Це особливо небезпечно для корпоративного сектору, де можуть використовуватися підроблені голосові або відеоповідомлення для обману співробітників.

Застосування AI та ML у кіберзлочинності значно підвищує складність і масштабність атак. Організаціям та користувачам необхідно адаптувати свої стратегії безпеки, впроваджувати інструменти для виявлення загроз, покращувати обізнаність персоналу та використовувати засоби багаторівневого захисту, щоб зменшити ризики, пов'язані з цими новими методами атак.

1.2.2 Вразливості пристроїв інтернет речей

Швидке зростання кількості пристроїв Інтернету речей (IoT) створює нові вразливості для кіберзагроз. Очікується, що до 2025 року їхня кількість перевищить 41 мільярд, що значно збільшить потенційні вектори атаки [9]. Багато IoT-пристроїв мають слабкі або взагалі відсутні механізми захисту, що робить їх привабливою мішенню для зловмисників. Хакери можуть використовувати вразливі пристрої для несанкціонованого доступу до мереж підприємств або особистих даних користувачів. Одним із поширених сценаріїв атаки є створення ботнетів, які складаються з

заражених IoT-пристроїв і можуть бути використані для DDoS-атак. Проблема посилюється тим, що багато користувачів не змінюють стандартні паролі або не оновлюють прошивки пристроїв. Відсутність єдиних стандартів безпеки для IoT-обладнання ускладнює розробку ефективних механізмів захисту. Організації повинні впроваджувати політики безпеки, що включають моніторинг мережевого трафіку та виявлення аномальної активності. Також важливим кроком є впровадження механізмів автентифікації та шифрування даних. Лише комплексний підхід до кіберзахисту допоможе зменшити ризики, пов’язані з використанням IoT-пристроїв.

1.2.3 Ransomware-as-a-Service (RaaS)

Професіоналізація кіберзлочинців сприяла появі платформ «Ransomware-as-a-Service» (RaaS), які дозволяють навіть малодосвідченим зловмисникам здійснювати складні атаки із застосуванням програм-вимагачів. Ця модель працює за принципом підписки або розподілу прибутку, де розробники шкідливого ПЗ надають свої інструменти іншим кіберзлочинцям [10]. У результаті, атаки програм-вимагачів стали більш доступними та масовими, що значно підвищило рівень загрози для компаній та звичайних користувачів. Завдяки RaaS навіть особи без глибоких технічних знань можуть запускати шифрувальні атаки на великі організації.

Жертви таких атак часто змушені сплачувати викуп, оскільки зловмисники блокують доступ до важливих даних. Крім того, багато платформ RaaS пропонують додаткові послуги, такі як технічна підтримка та оновлення шкідливого коду, що робить їх ще більш ефективними. Ця тенденція сприяє зростанню кількості атак на державні установи, лікарні та бізнеси, що може призводити до серйозних економічних збитків. Для протидії таким загрозам компанії повинні впроваджувати багаторівневий захист, включаючи резервне копіювання даних, сегментацію мережі та навчання персоналу. Також важливим є міжнародне співробітництво у сфері кібербезпеки для боротьби з RaaS-платформами та їх розробниками. Лише комплексні заходи можуть допомогти зменшити ризики, пов’язані з поширенням програм-вимагачів.

1.2.4 Використання хмарних сервісів та віддалена робота

Перехід на віддалену роботу та використання хмарних сервісів значно розширили вектори атак. Кіберзлочинці активно використовують слабкі місця у незахищених домашніх мережах для проникнення в корпоративні системи. Багато працівників працюють з особистих пристроїв, які не мають належного рівня безпеки, що підвищує ризик компрометації даних [11]. Також поширеною проблемою є неправильне налаштування хмарних сервісів, що може призводити до витоку конфіденційної інформації [12]. Хакери використовують такі вразливості для викрадення чутливих даних або порушення роботи організацій. Фішингові атаки стали ще більш ефективними, оскільки працівники частіше взаємодіють онлайн, а відсутність безпечного корпоративного середовища спрощує обман. Крім того, кіберзлочинці застосовують атаки «людина посередині» (MITM), перехоплюючи незашифрований трафік у відкритих або домашніх Wi-Fi-мережах. Зловмисники також активно експлуатують вразливості VPN, які стали основним засобом підключення до корпоративних ресурсів. Для захисту компанії повинні впроваджувати політики безпечного доступу, такі як багатофакторна автентифікація та шифрування трафіку. Важливим є також навчання персоналу, щоб запобігти компрометації акаунтів через соціальну інженерію.

1.2.5 Криптоджекінг та атаки на криптовалютні платформи

Кіберзлочинці продовжують використовувати шкідливе програмне забезпечення для прихованого майнінгу криптовалют на чужих пристроях. У деяких регіонах, зокрема в Індії, їх кількість зросла на 409% [13]. Це призводить до зниження продуктивності систем, підвищеного споживання електроенергії та швидкого зношування обладнання [14].

Крім того, шахраї активно експлуатують криптовалютні платформи для фінансових махінацій. Вони використовують фальшиві біржі, фішингові сайти та схеми швидкого збагачення, щоб викрадати кошти користувачів. Часто жертвами

таких атак стають новачки, які не мають достатніх знань про безпечне використання криптовалют. Використання анонімних транзакцій ускладнює відстеження зловмисників та повернення втрачених коштів. Усвідомленість користувачів і сучасні засоби кіберзахисту є ключовими елементами протидії шахрайству з криптовалютами.

Організації розгортають багаторівневі системи безпеки для захисту від нових загроз, але така складність може призвести до прогалин у покритті або неефективності. Оскільки кіберзагрози випереджають захисні заходи, компанії намагаються ефективно інтегрувати свої інструменти та постійно впроваджують нові технології [15].

Швидка цифровізація інфраструктури створила складний ландшафт кібербезпеки, в якому вразливості хмарних сервісів, систем IoT та віддалених робочих середовищ використовуються все більш винахідливими зловмисниками.

Щоб зменшити ці ризики, організації повинні впроваджувати інтегровані стратегії кібербезпеки, які включають сучасні інструменти виявлення загроз, ефективні навчальні програми для співробітників і суворі політики управління пристроями.

1.3 Втрати організацій від кібератак

Наслідки кібератак можуть виходити далеко за межі виключно фінансових втрат. Вони можуть впливати на репутацію компанії, її конкурентоспроможність, правову відповідальність та навіть безпеку співробітників і клієнтів.

Усі ці витрати можуть суттєво вплинути на фінансовий стан компанії, репутацію та довіру клієнтів. Тому ефективна система кібербезпеки та стратегія реагування на інциденти є критично важливими для мінімізації ризиків. Однак для захисту від таких ризиків компаніям необхідно не лише інвестувати в кібербезпеку, а й впроваджувати стратегії постійної перевірки заходів що застосовуються.

Розглянемо основні категорії втрат, які можуть виникнути внаслідок кібератак [16, 17, 18].

1.3.1 Фінансові втрати

Кібератаки можуть безпосередньо призводити до фінансових збитків через крадіжку коштів, витрати на ліквідацію наслідків та втрату прибутків. Середні збитки від зламу в 2024 складали $4.88 мільйони, що на 10% більше ніж в 2023 році [19].

- Прямі витрати, що виникають у разі кібератаки, включають значні фінансові виплати, необхідні для відновлення роботи компанії. Сюди належать витрати на відновлення систем, що можуть включати оновлення серверів, мережевої інфраструктури, баз даних та програмного забезпечення. Якщо атака спричинила втрату або пошкодження даних, додаткові ресурси витрачаються на їхнє відновлення. Також компанії змушені залучати експертів із реагування на інциденти, цифрової криміналістики та кібербезпеки, які аналізують наслідки атаки, визначають її джерела та розробляють заходи для запобігання подібним інцидентам у майбутньому. Окрім цього, юридичні консультації стають необхідністю, особливо якщо компанія може зазнати судових позовів або повинна дотримуватися нормативних вимог щодо конфіденційності даних.

- Витрати на компенсацію є ще одним важливим аспектом фінансових втрат, оскільки компанії можуть бути змушені відшкодовувати збитки клієнтам або партнерам. У разі витоку персональних або фінансових даних постраждалим часто пропонують компенсації або інші безкоштовні послуги. Якщо порушення безпеки вплинуло на діяльність партнерських компаній, вони можуть висувати вимоги про компенсацію за понесені збитки або втрати, що виникли через зупинку бізнес-процесів.

- Окремим і серйозним наслідком є штрафи та санкції, які можуть бути накладені регуляторами у випадку порушення вимог нормативних актів. Наприклад, витік персональних даних може стати підставою для значних штрафів згідно з європейським регламентом GDPR. Фінансові, медичні та державні установи також зобов’язані дотримуватися галузевих стандартів безпеки, і їхнє порушення може призвести до суттєвих санкцій та репутаційних втрат.

• Кібератаки часто спричиняють втрату прибутків через простої, особливо якщо вони блокують роботу бізнесу. Онлайн-сервіси можуть стати недоступними, що безпосередньо впливає на продажі та фінансові операції. Для промислових підприємств це може означати зупинку виробничих процесів і значні матеріальні втрати. Додатково до цього, відтік клієнтів після інциденту є поширеним явищем, оскільки довіра до компанії значно знижується, а конкуренти можуть скористатися цією ситуацією для залучення нових користувачів.

• Ще одним видом фінансових втрат є збитки від крадіжки коштів. У деяких випадках хакери отримують прямий доступ до банківських рахунків компанії, здійснюючи незаконні транзакції. Використання методів соціальної інженерії може призвести до того, що співробітники помилково переказують значні суми на рахунки зловмисників, наприклад, у випадку шахрайських електронних листів, що імітують запити від керівництва чи партнерів. Крім того, значну загрозу становлять атаки із використанням шифрувального програмного забезпечення, коли зловмисники блокують доступ до даних і вимагають викуп за їхнє розшифрування.

1.3.2 Втрата даних та інтелектуальної власності

Важливо також враховувати втрати, отримані внаслідок викрадення важливих для компанії даних [20].

Витік персональних даних клієнтів або співробітників створює серйозні ризики, оскільки зловмисники можуть використовувати їх для шахрайства, крадіжки особистості або вимагання викупу. Фінансова інформація, така як номери кредитних карток або банківські реквізити, може бути використана для незаконних транзакцій. Доступ до електронної пошти або акаунтів у соціальних мережах дозволяє хакерам поширювати шкідливе програмне забезпечення або маніпулювати жертвами. Викрадені персональні дані також можуть бути продані на чорному ринку або використані для створення підроблених документів.

Викрадення конфіденційної бізнес-інформації може суттєво підірвати конкурентні переваги компанії та спричинити фінансові втрати. Зловмисники можуть

отримати доступ до унікальних технологій, розробок, бізнес-стратегій або комерційних переговорів, що дасть конкурентам можливість використати цю інформацію у власних цілях. Викрадені патенти, формули або виробничі процеси можуть бути продані або використані для створення аналогічних продуктів без значних витрат на дослідження та розробку. Інформація про клієнтів та постачальників також може бути скомпрометована, що загрожує втратою партнерських відносин. Витік стратегічних планів може вплинути на вартість компанії, особливо якщо вона публічно торгується на біржі.

Кібератаки можуть спричинити не лише крадіжку інформації, але й її знищення або навмисну модифікацію, що призводить до серйозних наслідків для бізнесу. Втрата критично важливих даних, таких як фінансові записи, операційна документація або база клієнтів, може паралізувати діяльність компанії. Зловмисники можуть змінювати дані з метою дезінформації або дискредитації, що особливо небезпечно для державних органів, фінансових установ і медичних закладів. Атаки на цілісність інформації можуть використовуватися для маніпулювання фінансовими звітами або підриву довіри до компанії.

1.3.3 Репутаційні втрати

Що стосується репутаційних втрат, кіберінциденти, пов’язані з витоком даних або компрометацією системи безпеки, можуть спричинити масовий відтік клієнтів [21]. Споживачі часто обирають компанії, яким довіряють, і будь-який сумнів щодо безпеки їхніх персональних даних може змусити їх звернутися до конкурентів. Особливо це стосується фінансових установ, e-commerce платформ і сервісів, що обробляють конфіденційну інформацію. Втрата клієнтів призводить до зниження прибутків, що ускладнює подальший розвиток бізнесу та змушує компанію витрачати значні кошти на відновлення довіри. Репутаційні ризики можуть мати довготривалий ефект, і навіть після впровадження посилених заходів безпеки частина клієнтів може більше не повернутися. Відновлення позицій на ринку потребує активних маркетингових кампаній, що також супроводжується додатковими витратами.

Бізнес-партнери розраховують на безпечну співпрацю, і якщо компанія демонструє вразливість до кіберзагроз, це може вплинути на довгострокові ділові відносини. Витік комерційної інформації або інциденти, що ставлять під загрозу безпеку спільних проектів, можуть змусити партнерів розірвати угоди або переглянути умови співпраці на жорсткіших умовах. Зокрема, постачальники та фінансові установи можуть вимагати додаткових гарантій безпеки або збільшити страхові внески для покриття можливих ризиків. У деяких випадках компанії можуть бути виключені з тендерів через нездатність забезпечити належний рівень захисту інформації. Втрата партнерів негативно впливає на фінансову стабільність, а пошук нових контрагентів потребує часу та додаткових ресурсів. Це також може знизити конкурентоспроможність компанії на ринку.

Кібератаки, особливо масштабні витоки даних, часто привертають увагу засобів масової інформації, що може мати довготривалий вплив на репутацію компанії. Публікації в новинних ресурсах, соціальних мережах і блогах можуть формувати негативний імідж, навіть якщо компанія швидко реагує та вживає необхідних заходів. Чим більший бізнес і кількість постраждалих клієнтів, тим масштабнішою стає медійна хвиля, що може призвести до публічного тиску та вимог від споживачів щодо компенсацій. Негативний інформаційний фон ускладнює залучення нових клієнтів і партнерів, а також впливає на вартість акцій компанії, якщо вона є публічною. У деяких випадках компанії доводиться інвестувати значні кошти в антикризовий PR, юридичний захист і заходи з відновлення довіри. Незважаючи на всі зусилля, деякі споживачі та інвестори можуть більше не розглядати компанію як надійного гравця на ринку.

1.3.4 Юридична та регуляторна відповідальність

Після витоку персональних даних клієнти, які постраждали від атаки, можуть подати позови до суду, вимагаючи компенсацію за завдані збитки. Вони можуть вимагати відшкодування витрат на виправлення наслідків шахрайства, а також моральної шкоди через порушення їхньої приватності. Компанії доведеться покрити

витрати на юридичний захист, а також на можливі виплати компенсацій. Окрім фінансових збитків, це може призвести до ще більшого падіння довіри до бренду та зниження лояльності клієнтів. Позови можуть зайняти тривалий час, і їх результат може бути непередбачуваним, що створює додаткові ризики для бізнесу. У разі великомасштабних інцидентів ці позови можуть стати колективними, що значно збільшує загальний розмір претензій.

Компанії, що порушують норми щодо захисту даних, можуть зазнати санкцій з боку регулюючих органів. У разі витоку персональних даних або іншої інформації, що підлягає захисту згідно з такими стандартами, як GDPR, CCPA чи іншими місцевими законами, органи влади можуть накладати значні штрафи [22]. Ці санкції можуть варіюватися залежно від тяжкості порушення та кількості постраждалих осіб. Крім штрафів, регулятори можуть вимагати впровадження негайних змін у політиках безпеки, що потребує додаткових витрат та часу на виконання вимог. Для деяких компаній штрафи можуть стати катастрофічними, особливо якщо вони вже мають попередні порушення або були попереджені про потенційні ризики. Це не лише впливає на фінансовий стан, але й на репутацію компанії на ринку.

У разі серйозних порушень безпеки та нехтування обов'язковими заходами захисту даних, керівництво компанії може бути притягнуте до кримінальної відповідальності. Якщо буде доведено, що компанія свідомо ігнорувала вимоги законодавства або не вжила необхідних заходів для захисту даних, це може призвести до судових процесів проти осіб, відповідальних за безпеку. Це створює додатковий юридичний та репутаційний ризик для організації, і навіть якщо покарання не буде жорстким, сам процес може забрати багато ресурсів та часу.

1.3.5 Соціальні та психологічні наслідки

Кібератаки можуть вплинути не лише на компанію, а й на її співробітників і клієнтів.

Після кібератаки працівники, які займаються кібербезпекою, можуть працювати в умовах високого стресу, оскільки потрібно терміново реагувати на

інцидент, виявляти та усувати загрози, відновлювати системи та забезпечувати безпеку [23]. Кризовий режим роботи може тривати кілька днів чи навіть тижнів, що підвищує ризик вигорання серед співробітників. Постійний тиск, відсутність нормального робочого часу та необхідність працювати понаднормово можуть негативно позначитися на психоемоційному стані персоналу. Це не тільки знижує ефективність роботи, але й збільшує ймовірність помилок. Важливою є підтримка з боку керівництва та вжиття заходів для мінімізації стресових ситуацій, таких як забезпечення належного відпочинку та організація постійної психологічної допомоги. Проблеми з вигоранням можуть призвести до високої плинності кадрів та втрати кваліфікованих фахівців.

Після кожної кіберзагрози компанії часто вимушені організовувати додаткове навчання для своїх співробітників, аби підвищити рівень обізнаності щодо нових загроз та удосконалити навички реагування на них. Оскільки кіберзагрози постійно еволюціонують, важливо, щоб працівники постійно отримували актуальну інформацію та навички для ефективної боротьби з новими типами атак. Цей процес займає значні ресурси як в часі, так і фінансово, адже для підвищення кваліфікації персоналу може знадобитися залучення зовнішніх експертів або проведення серії тренінгів. Додатково, навчання покращує загальну кіберграмотність серед співробітників, знижуючи ризик внутрішніх загроз та підвищуючи ефективність заходів з безпеки. Ретельно сплановане навчання також дозволяє створити культуру безпеки в компанії, де кожен працівник активно сприяє збереженню конфіденційності та безпеки даних.

1.4 Вимоги міжнародних та державних стандартів до тестування кібербезпеки

Оскільки міжнародні та державні стандарти в більшій мірі визначають як саме організації повинні будувати свої системи захисту (СЗ), важливо розглянути конкретні вимоги до тестування безпеки інформаційних систем та які вимоги

висуваються до перевірки захищеності. Розглянемо деякі розповсюджені стандарти, які широко використовуються у світі.

- ISO/IEC 27001 [24]:

ISO 27001 підкреслює важливість тестування безпеки як частини процесу управління ризиками. Хоча стандарт не вимагає безпосередньо проведення тестування на проникнення, він рекомендує оцінку вразливостей та виконання тестування безпеки на етапі розробки (контролі A.12.6.1 та A.8.29). Тестування на проникнення дозволяє виявити слабкі місця в системі до того, як вони можуть бути використані зловмисниками, що є критично важливим для забезпечення належного рівня захисту інформації та підтримки відповідності вимогам ISO 27001. Важливо, щоб тестування безпеки стало частиною постійного циклу оцінки та покращення захисту інформаційних систем, що відповідає принципам цього стандарту.

ISO 27001 не встановлює конкретних вимог щодо частоти проведення тестів на проникнення, проте в галузі є загальноприйнята рекомендація проводити їх мінімум двічі на рік для забезпечення належної відповідності вимогам. Ця практика дозволяє своєчасно виявляти нові вразливості, що можуть з’явитися внаслідок змін у технологіях, програмному забезпеченні чи структурах інформаційної системи. Періодичне тестування дозволяє зберігати високий рівень безпеки, забезпечувати оперативне реагування на нові загрози та підтримувати відповідність стандартам безпеки, таким як ISO 27001, у межах організації.

Обсяг тестування на проникнення в контексті ISO 27001 передбачає чітке визначення, які цифрові активи підлягають тестуванню, а також вказівку на можливі виключення та інші важливі аспекти, що слід враховувати до проведення тестування. Приділення уваги цим аспектам важливе для запобігання впливу на критичні бізнес-процеси та для забезпечення того, щоб тестування охоплювало всі важливі компоненти системи безпеки.

- PCI DSS [25]:

PCI DSS вимагає регулярного тестування безпеки, що включає як щоквартальні зовнішні та внутрішні сканування вразливостей, так і щорічне тестування на проникнення (Вимога 11) [26]. Це забезпечує виявлення та усунення потенційних

вразливостей, що можуть бути використані зловмисниками для отримання несанкціонованого доступу до чутливої інформації, такої як дані карток. Регулярне тестування є невід'ємною частиною підтримки високого рівня безпеки, необхідного для відповідності стандарту PCI DSS, і дає можливість своєчасно виявляти нові загрози, що виникають у результаті змін у системах або технологіях.

PCI DSS вимагає проведення тестування за певною частотою:

- Вони проводяться кожні три місяці. Зовнішнє сканування виконується через Approved Scanning Vendor (ASV), сертифікованого постачальника послуг сканування, а внутрішні сканування можуть бути здійснені безпосередньо компанією. Це дозволяє своєчасно виявити нові вразливості в мережах і системах, що можуть бути використані для атак на інформаційні активи компанії.
- Тестування має проводитися хоча б раз на рік для імітації реальних кібератак. Метою є виявлення слабких місць у системах, мережах і додатках, які обробляють або передають дані карток, що допомагає оцінити рівень захисту від атак, таких як експлуатація вразливостей, які не були виявлені під час інших тестів.

Обсяг тестування на проникнення за стандартом PCI DSS включає як зовнішнє, так і внутрішнє ТС, мереж і додатків, що зберігають, обробляють або передають дані карток [27]. Це охоплює всі компоненти інфраструктури, які мають доступ до чутливих даних, і забезпечує всебічний підхід до виявлення потенційних загроз. Тестування повинно проводитись для всіх частин системи, які можуть впливати на безпеку даних карток, щоб мінімізувати ризик витоку або компрометації цієї інформації.

- GDPR [28]:

GDPR (Загальний регламент захисту даних) не вимагає конкретно проведення регулярного тестування безпеки, такого як тестування на проникнення. Однак він зобов'язує організації впроваджувати відповідні технічні та організаційні заходи для забезпечення захисту персональних даних (Стаття 32) [29]. Включаючи заходи безпеки, які мають бути достатніми для запобігання несанкціонованому доступу, втраті чи пошкодженню персональних даних. Вимога щодо захисту даних не обмежується лише технічними рішеннями, а також передбачає організаційні заходи,

такі як навчання персоналу та створення політик безпеки, які допомагають запобігти порушенням конфіденційності даних.

GDPR не встановлює конкретних вимог щодо частоти або обсягу тестування безпеки. Однак, організації повинні регулярно переглядати та оновлювати свої заходи безпеки, щоб переконатися, що вони достатні для захисту персональних даних. Це означає, що організації повинні адаптувати свої безпекові політики та практики до змін у загрозах, технологіях та законодавстві. Регулярний перегляд та адаптація заходів безпеки можуть включати проведення тестів на проникнення або інших видів тестування для перевірки наявних вразливостей, хоча ці дії не прописані безпосередньо в самому регламенті. Важливо, щоб організації забезпечували належний рівень захисту даних і могли продемонструвати це у разі перевірки або в разі порушення.

Також варто розглянути які вимоги до регулярного тестування безпеки організацій висуває українське законодавство.

Українське законодавство містить згадки про перевірку впроваджених заходів захисту інформації, що включають регулярне ТС захисту. Зокрема, нормативні документи, такі як НД ТЗІ 2.3-025-24 [30], визначають методику оцінювання заходів захисту інформації. Крім того, НД ТЗІ 2.1-002-07 [31] встановлює загальні вимоги до організації проведення випробувань комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Ці випробування є невід'ємною частиною процесу атестації комплексів технічного захисту інформації та забезпечують відповідність встановленим вимогам щодо захисту інформації з обмеженим доступом. Також, відповідно до ДСТУ 3396.0-96 [32], керування системою захисту інформації включає регулярний аналіз функціонування системи та адаптацію заходів захисту до поточних умов, що може включати регулярне тестування. Також, Порядок проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури [33] передбачає оцінку стану інформаційної безпеки на відповідність вимогам законодавства у сферах кібербезпеки та захисту інформації. Цей аудит включає тестування на проникнення як метод оцінювання захищеності інформаційних систем шляхом імітації несанкціонованого втручання в їх роботу.

Таким чином, українське законодавсто вимагає оцінки та перевірки ефективності систем захисту інформації, однак воно не встановлює конкретних вимог щодо частоти тестування.

Проаналізувавши міжнародні та українські вимоги, що стосуються ТС захисту які впроваджені в організації, можна зробити висновок що вони потребують більш чіткого визначення, а також вимог щодо постійного тестування, оскільки зміни в СЗ вносяться ледь не щоденно, як результат – перевірки, які здійснюються здебільшого раз в пів року, не можуть гарантувати організаціям що їхні СЗ працюють коректо протягом всього часу.

1.5 Традиційні методи тестування кібербезпеки

У цьому підрозділі розглядаються класичні підходи до перевірки рівня захисту організацій та їхні особливості.

У сфері інформаційної безпеки організації застосовують різні методи для оцінки та підвищення рівня захисту своїх інформаційних систем. Одним з найбільш поширених є тестування на проникнення (пентест), яке передбачає симуляцію атак з метою виявлення вразливостей. Розглянемо детальніше методологію пентесту, його етапи та обмеження.

Методологія пентесту ґрунтується на систематичному підході до виявлення та експлуатації вразливостей в інформаційних системах [34]. Існують різні методології пентесту, кожна з яких має свої особливості та підходи до проведення тестування.

Основні етапи пентесту [35, 36]:

1. Збір інформації: На цьому етапі тестувальники збирають дані про цільову систему, такі як мережеві адреси, доменні імена, інформацію про сервери та інші деталі, які можуть допомогти в подальшому тестуванні.

2. Аналіз вразливостей: Після збору інформації проводиться аналіз на предмет можливих вразливостей, використовуючи автоматизовані інструменти та ручні методи для виявлення слабких місць у системі.

3. Експлуатація: На цьому етапі тестувальники намагаються використати виявлені вразливості для отримання несанкціонованого доступу до системи або її компонентів.

4. Пост-експлуатація: Після успішної експлуатації тестувальники оцінюють можливості збереження доступу, розширення привілеїв та інші аспекти, які можуть бути використані зловмисниками.

5. Звітність: Підготовка детального звіту про проведене тестування, включаючи виявлені вразливості, методи їх експлуатації та рекомендації щодо їх усунення.

Обмеження пентесту [37]:

- Часові обмеження: Тестування зазвичай проводиться в обмежений проміжок часу, що може вплинути на глибину та повноту перевірки.
- Залежність від навичок команди: Ефективність пентесту значною мірою залежить від досвіду та кваліфікації тестувальників.
- Фокус на конкретних векторах атаки: Пентест може бути спрямований на певні аспекти системи, що може залишити інші потенційно вразливі ділянки непоміченими.

Розуміння цих етапів та обмежень є ключовим для ефективного використання пентесту як інструменту оцінки та підвищення рівня інформаційної безпеки організації.

Також серед основних методів виділяють Red Teaming. Основна відмінність між пентестом та Red Teaming полягає в обсязі та підході до тестування безпеки. Пентест (тестування на проникнення) є більш вузьконаправленим і технічним, зосереджуючись на виявленні конкретних вразливостей у системах, в той час як Red Teaming є більш комплексним підходом, який оцінює загальний рівень безпеки організації [38]. Це включає не лише технічні аспекти, але й оцінку фізичної безпеки, здатності персоналу реагувати на інциденти та ефективність процедур реагування. Red Teaming імітує реальні атаки з боку зловмисників, використовуючи різноманітні тактики, техніки та процедури для оцінки загальної готовності організації до кіберзагроз [39].

В сфері інформаційної безпеки Red Teaming є методикою, що передбачає симуляцію атак з боку етичних хакерів для оцінки ефективності захисних заходів організації. Цей підхід дозволяє виявити вразливості та оцінити здатність персоналу реагувати на реальні загрози.

Розглянемо переваги Red Teaming:

- Реалістична оцінка безпеки: Red Teaming імітує дії справжніх зловмисників, що дозволяє виявити слабкі місця в системах, мережах та фізичній безпеці організації [40].
- Покращення реакції на інциденти: Процес тестування допомагає оцінити ефективність команд реагування на інциденти, виявляючи можливості для покращення процедур та навчання персоналу [41].
- Ідентифікація комплексних загроз: Red Teaming дозволяє виявити складні та багатоступінчасті атаки, які можуть бути непомітними для традиційних методів тестування [42].
- Покращення культури безпеки: Регулярні симуляції атак підвищують обізнаність співробітників щодо потенційних загроз та сприяють формуванню культури безпеки в організації [43].

Що стосується недоліків Red Teaming, серед них можна виділити наступні:

1. Обмежене охоплення: Red Teaming може зосереджуватися на конкретних аспектах безпеки, що може залишити інші вразливості непоміченими [44].
2. Значні трудовитрати: Процес може бути трудомістким та дорогим, вимагаючи значних ресурсів для планування, виконання та аналізу результатів [45].
3. Можливий вплив на операційну діяльність: Симуляції атак можуть вплинути на нормальну роботу систем та процесів, що потребує ретельного планування та координації.
4. Етичні та правові питання: Проведення тестів може викликати етичні та правові питання, особливо якщо симуляції включають фізичні вторгнення або інші потенційно спірні методи.

Загалом, Red Teaming є потужним інструментом для оцінки та покращення безпеки організації, але його слід застосовувати з обачністю, враховуючи потенційні ризики та обмеження.

Наступними варто розглянути внутрішні аудити безпеки та їх ефективність. Внутрішні аудити безпеки є невід'ємною частиною системи управління інформаційною безпекою в організації. Вони сприяють виявленню потенційних загроз, оцінці ефективності існуючих заходів безпеки та забезпеченню відповідності нормативним вимогам.

Як компанії проводять аудити безпеки

Компанії застосовують різні методи для проведення внутрішніх аудитів безпеки, зокрема [46, 47]:

- Регулярний аналіз логів: Огляд журналів подій допомагає виявляти підозрілі дії, несанкціоновані доступи та інші аномалії в системах.
- Перевірка політик доступу: Аудит політик доступу забезпечує контроль за тим, хто має доступ до яких ресурсів, та чи відповідає цей доступ ролям і обов'язкам співробітників.
- Оцінка відповідності стандартам: Перевірка відповідності міжнародним стандартам, таким як ISO 27001, допомагає оцінити рівень зрілості системи управління інформаційною безпекою.
- Огляд мережевої інфраструктури: Аналіз мережевої архітектури та конфігурацій допомагає виявляти потенційні вразливості та забезпечувати належний рівень захисту даних.
- Оцінка управління ризиками: Визначення та аналіз ризиків дозволяють виявляти потенційні загрози та вразливості, що можуть вплинути на безпеку інформації.

Завдяки цим заходам, внутрішній аудит сприяє виявленню недоліків у системі безпеки та наданню рекомендацій щодо їх усунення.

Незважаючи на регулярність та систематичність внутрішніх аудитів, вони іноді не здатні виявити складні або новітні загрози через кілька причин [48]:

- Обмежена глибина аналізу: Внутрішні аудитори можуть не мати достатньої експертизи або ресурсів для глибокого аналізу складних загроз, особливо якщо вони є новими або маловідомими.
- Фокус на відповідності: Аудити часто зосереджуються на перевірці відповідності стандартам та політикам, що може відволікати від пошуку нових або невідомих загроз.
- Використання стандартних тестів: Стандартні методи тестування можуть не охоплювати всі можливі вектори атак, особливо якщо зловмисники використовують новітні або нетрадиційні методи.
- Недостатнє оновлення методологій: Якщо методи та інструменти аудиту не оновлюються відповідно до нових загроз, це може призвести до пропуску атак.
- Обмежені ресурси: Недостатнє фінансування або кадрові ресурси можуть обмежувати можливості проведення глибоких та всебічних аудитів.

1.6 Недоліки традиційних підходів до тестування безпеки

Розглянемо основні недоліки традиційних підходів до тестування безпеки організації:

- **Обмежена частота перевірок:**

Традиційні підходи до перевірки безпеки, зокрема пентести, зазвичай проводяться лише 1-2 рази на рік [49]. Така рідкість перевірок робить ці методи недостатньо ефективними для забезпечення безпеки організації. Кіберзагрози постійно еволюціонують, з'являються нові вектори атак та вразливості, як результат – час між перевірками може бути критичним для виявлення цих загроз. За цей час організації можуть стати мішенями для нових видів атак, яких пентест навіть не враховує через обмежений часовий інтервал між тестуваннями. Таким чином, відсутність регулярних перевірок ускладнює своєчасну адаптацію до загроз.

- **Висока залежність від людського фактора:**

Якість проведення пентестів та аудиту безпеки значною мірою залежить від кваліфікації і досвіду конкретних фахівців [50]. Ручні перевірки вразливостей, навіть

найретельніші, можуть пропустити нові або нетипові загрози, які не були б виявлені за допомогою стандартних інструментів. Людський фактор також сприяє виникненню помилок, адже спеціалісти можуть не виявити нестандартні комбінації атак або пропустити певні вразливості через обмеженість знань чи досвіду в специфічних галузях. Крім того, навіть досвідчені пентестери не можуть перевірити всі можливі сценарії атак, що створює простір для невиявлених загроз.

- **Неможливість автоматизованої перевірки великої кількості сценаріїв:**

Традиційні методи тестування безпеки не можуть ефективно імітувати сотні потенційних векторів атак одночасно. Багато пентестерів або спеціалістів з безпеки працюють вручну, що обмежує їх здатність перевіряти різноманітні сценарії в обмежений час. Автоматизація тестувань стала важливим напрямком у кібербезпеці, адже дозволяє охоплювати більший обсяг перевірок без значних затрат часу та зусиль. Інструменти автоматизованого тестування здатні запускати численні сценарії одночасно, що значно покращує виявлення нових вразливостей і підвищує загальний рівень безпеки організації.

- **Висока вартість повноцінного тестування для організацій:**

Проведення повноцінного тестування, особливо Red Teaming або глибокого пентесту, є дорогим і трудомістким процесом. Для деяких компаній вартість таких послуг може бути непосильним фінансовим навантаженням. Організації часто змушені обмежувати кількість перевірок або проводити їх на менш глибокому рівні через відсутність фінансових ресурсів [51]. Це може знижувати ефективність системи безпеки, оскільки частота тестувань і їхня глибина мають безпосередній вплив на здатність компанії виявляти та нейтралізувати потенційні загрози.

- **Значний часовий розрив між перевіркою та фактичним усуненням виявлених проблем:**

Однією з суттєвих проблем традиційних підходів є значний часовий розрив між виявленням вразливості та її усуненням [52]. В середньому організаціям потрібно від 60 до 150 днів на усунення вразливості [53]. Після пентесту або аудиту безпеки компанії часто потребують кількох місяців для виправлення знайдених проблем, що створює ризик використання цих вразливостей зловмисниками. За цей час

зловмисники можуть скористатися знайденими проблемами, щоб здійснити атаки, завдати збитків або отримати несанкціонований доступ до конфіденційної інформації. Крім того, в деяких випадках компанії можуть просто не встигнути усунути всі знайдені вразливості до того, як зловмисники вдадуться до атаки.

1.7 Розширення цифрової інфраструктури організацій

Розширення цифрової інфраструктури принесло численні переваги, але також створило значні вразливості. Інфрастуктури організацій стали більш децентралізовані [54], а кількість систем захисту значно зросла для підтримки безпеки всієї розподіленої інфраструктури.

Організації зазвичай використовують різноманітні системи безпеки для захисту своїх активів, даних та персоналу. Кількість і типи цих систем можуть значно варіюватися залежно від розміру організації, галузі та специфічних потреб безпеки. Загальні заходи безпеки включають:

— Брандмауери, антивірусне програмне забезпечення, системи виявлення вторгнень та технології шифрування для захисту цифрових активів.

— Системи управління ідентифікацією та доступом (IAM): для контролю та моніторингу доступу користувачів до критичних систем і даних.

— Системи управління подіями безпеки (SIEM): для аналізу в режимі реального часу сповіщень про безпеку, що генеруються апаратними та програмними засобами.

Згідно з опитуванням, проведеним журналом Infosecurity Magazine в 2021 році, організації в середньому використовують 76 інструментів безпеки, що на 19% більше, ніж за попередні два роки [55]. Причому великі компанії можуть використовувати понад 130 систем захисту [56]. Важливо зазначити, що ефективність цих систем безпеки залежить не лише від їхньої кількості, але й від їхньої інтеграції та від того, наскільки добре вони узгоджуються із загальною стратегією безпеки організації. Регулярні оцінки та оновлення мають вирішальне значення для усунення нових загроз і вразливостей.

1.8 Потреба у нових підходах до тестування кібербезпеки

У сучасному цифровому середовищі кіберзагрози постійно еволюціонують, що вимагає від організацій адаптації та вдосконалення підходів до кіберзахисту.

Зростання кількості та складності загроз вимагає від компаній впровадження новітніх технологій та дотримання актуальних стандартів безпеки [57]. Періодичні перевірки можуть бути недостатніми для виявлення новітніх загроз. Безперервне тестування, зокрема через моделювання атак, дозволяє оперативно виявляти та реагувати на потенційні вразливості [58].

Автоматизовані системи моделювання атак імітують можливі шляхи атак та методи, які використовують зловмисники, забезпечуючи безперервний моніторинг та тестування безпеки. Симуляція атак є безперервним автоматизованим тестом на проникнення, який імітує реальні методи атак зловмисників, надаючи більш точну оцінку рівня захищеності системи.

Брак чіткого розуміння переваг та комплексного підходу до симуляції атак призводить до сприйняття таких рішень як одноразових, що обмежує їхню ефективність у довгостроковій перспективі.

Розуміння та впровадження безперервного тестування та симуляції атак є ключовими для адаптації до швидко змінюваного ландшафту кіберзагроз, забезпечуючи проактивний підхід до захисту інформаційних систем.

Висновки до першого розділу

Зростаюча кількість і складність кібератак в Україні та світі, зокрема на критичну інфраструктуру, підкреслюють необхідність постійного вдосконалення заходів кібербезпеки. Симуляція кібератак (СК), як частина безперервного тестування, є важливою складовою традиційних методів, забезпечуючи проактивний підхід до виявлення та нейтралізації потенційних загроз.

Кіберзлочинці значно вдосконалили свої методи, використовуючи штучний інтелект для автоматизації атак, що ускладнює їх виявлення та нейтралізацію.

Зростання кількості вразливих IoT-пристроїв, використання Ransomware-as-a-Service та розширення векторів атак через хмарні сервіси і віддалену роботу створюють нові виклики для кібербезпеки.

Кібератаки можуть призвести до значних фінансових втрат, репутаційних збитків і юридичних наслідків, що серйозно впливають на діяльність компанії. Для мінімізації цих ризиків необхідно не лише інвестувати в кібербезпеку, а й регулярно перевіряти ефективність вжитих заходів та стратегій реагування. Міжнародні та українські стандарти визначають важливість тестування безпеки інформаційних систем, але не завжди чітко встановлюють вимоги щодо частоти або обсягу таких перевірок. Тому є потреба в удосконаленні вимог для постійного тестування, щоб забезпечити ефективний захист в умовах регулярних змін у системах безпеки.

Традиційні методи тестування кібербезпеки, зокрема пентест та Red Teaming, мають свої переваги та обмеження. Пентест зосереджується на виявленні вразливостей конкретних систем, тоді як Red Teaming оцінює загальний рівень безпеки, включаючи реакцію на інциденти та фізичну безпеку. Внутрішні аудити безпеки допомагають організаціям виявляти недоліки в системах захисту. Однак традиційні підходи до тестування мають кілька суттєвих недоліків, таких як обмежена частота перевірок, висока залежність від людського фактору та неможливість автоматизованої перевірки великої кількості сценаріїв. Оскільки кіберзагрози постійно еволюціонують, організації потребують нових підходів до тестування, таких як безперервне тестування та моделювання атак.

РОЗДІЛ 2
СУЧАСНІ ПІДХОДИ ДО СИМУЛЯЦІЇ КІБЕРАТАК ТА ЇХ ЗАСТОСУВАННЯ

2.1. Концепція симуляції кібератак

З метою передбачити нові кібератаки, використовується моделювання кібератак, тобто створення такої моделі, що відображає реальні дії, аналогічні до кібератаки. Моделювання кібератак – це процес створення математичних, логічних, або імітаційних моделей, що відображають сценарії, характеристики, параметри, результати або наслідки кібератак [59].

Під симуляцією кібератак будемо розуміти імітацію реальних атак на інформаційні системи з метою тестування ефективності заходів захисту. При цьому за допомогою систем симуляції кібератак, такі дії можуть виконуватись автоматизовано. На відміну від традиційних методів, таких як пентестинг або аудит безпеки, цей підхід дозволяє відтворити динаміку реальних атак у контрольованих умовах, що сприяє глибшому розумінню можливих загроз і слабких місць системи.

Основні принципи симуляції кібератак включають:

1. **Реалістичність сценаріїв** – використання тактик, технік і процедур (TTP), які відповідають поведінці реальних зловмисників.

2. **Автоматизація процесу** – застосування спеціалізованих платформ, що дозволяють моделювати атаки з мінімальним людським втручанням.

3. **Повторюваність тестування** – можливість багаторазового виконання сценаріїв для оцінки змін у рівні безпеки після впровадження захисних заходів.

4. **Безпечність проведення** – виконання тестів у контрольованому середовищі без ризику порушення роботи критичних систем. Варто зазначити, що для проведення симуляцій кібератак використовуються вже відомі загрози. Однак з метою не нашкодити системі що перевіряється, в код шкідливої програми вносяться зміни, які полягають у виконанні зворотніх дій, котрі повертають систему до початкового стану.

2.2 Використання MITRE ATT&CK для моделювання тактик, технік та процедур атакуючих

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) — це глобальна база знань, яка описує поведінку зловмисників на основі реальних спостережень [60]. Вона включає в себе тактики (цілі атакуючих), техніки (методи досягнення цих цілей) та процедури (конкретні реалізації технік).

Використання MITRE ATT&CK дозволяє організаціям:

- **Моделювати можливі атаки**: Створювати сценарії, які відображають реальні дії зловмисників, що підвищує ефективність тестування системи безпеки.
- **Оцінювати поточний рівень захисту**: Визначати, які техніки можуть бути використані проти організації та наскільки ефективно вони можуть бути виявлені або заблоковані.
- **Розробляти стратегії захисту**: Фокусуватися на конкретних техніках та тактиках, що становлять найбільшу загрозу, та впроваджувати відповідні заходи протидії.

MITRE ATT&CK надає стандартизовану та детальну інформацію про поведінку зловмисників, що робить її ідеальною основою для автоматизованих систем симуляції атак. Завдяки цьому:

- Системи можуть автоматично генерувати та виконувати сценарії атак, базуючись на актуальних даних про загрози.
- Організації можуть оцінювати ефективність своїх заходів безпеки, порівнюючи результати симуляцій з відомими техніками та тактиками.
- Оскільки MITRE ATT&CK постійно оновлюється, автоматизовані системи можуть швидко адаптуватися до нових методів атак та забезпечувати актуальність тестування.

Таким чином, інтеграція MITRE ATT&CK у процеси симуляції кібератак забезпечує більш точне та ефективне моделювання тактик, технік та процедур атакуючих, що сприяє підвищенню доцільності такого тестування.

2.3 Різниця між симуляцією загроз та емуляцією супротивників

У сфері кібербезпеки існують два проактивні підходи до оцінки та підвищення рівня захисту інформаційних систем: симуляція загроз та емуляція супротивника**.** Хоча обидва методи спрямовані на виявлення вразливостей та покращення захисних механізмів, вони відрізняються за обсягом, методологією та цілями.

Розглянемо основні характеристики, що стосуються симуляції загроз [61]:

- Симуляція загроз зосереджується на типових методах атак, таких як фішинг, шкідливе програмне забезпечення, програми-вимагачі та інші поширені загрози. Це дозволяє оцінити, наскільки ефективно існуючі засоби безпеки можуть протистояти цим загрозам.
- Під час симуляції загроз перевіряється ефективність таких засобів захисту, як міжмережеві екрани, системи виявлення та запобігання вторгнень (IDS/IPS), засоби захисту кінцевих точок (EDR) тощо. Мета — визначити, наскільки ці засоби здатні виявляти та блокувати поширені вразливості.
- Для постійної валідації захисту застосовуються платформи для моделювання атак (Breach and Attack Simulation, BAS). Ці інструменти автоматизують процес тестування, забезпечуючи безперервний моніторинг та оцінку ефективності засобів безпеки [62].
- Основна ціль симуляції загроз — виявлення системних слабких місць в інфраструктурі організації та забезпечення загального зміцнення безпеки.

Прикладом може бути імітація атаки програми-вимагача для оцінки ефективності захисту кінцевих точок.

Емуляція супротивника — це цільовий підхід, що відтворює конкретні тактики, техніки та процедури (TTP) реальних кіберзлочинців або груп, базуючись на реальній розвідці про відомі загрози, такі як передові постійні загрози (APT) або державні хакери [63].

Ключові характеристики емуляції супротивника наступні:

- Емуляція супротивника використовує дані про відомі загрози, такі як розвинені постійні загрози (APT) або державні хакери. Це дозволяє створювати сценарії атак, які максимально наближені до реальних дій зловмисників.
- У процесі емуляції супротивника часто залучаються спеціалізовані команди (Red Team), які імітують поведінку конкретних атакуючих, включаючи соціальну інженерію, методи бічного переміщення та інші складні техніки.
- Емуляція супротивника дозволяє перевірити, як захист витримує адаптовані, витончені атаки, що характерні для конкретних зловмисників. Це допомагає оцінити готовність організації до реальних загроз високого рівня.
- Основна ціль емуляції супротивника — валідація можливостей виявлення та реагування на високоточні загрози, а також підвищення готовності до реальних атак.

Прикладом може бути емуляція TTP групи APT29 (Cozy Bear) [64] для перевірки захисту від атак, що спонсоруються державами. Cozy Bear (APT29) — це угруповання кіберзлочинців, яке пов’язують з російськими спецслужбами, зокрема Службою зовнішньої розвідки (СЗР РФ). Відоме з 2008 року, група спеціалізується на шпигунстві проти урядових, дипломатичних і оборонних структур. Cozy Bear використовує складні методи фішингу, бекдори, а також уникає виявлення шляхом ретельного маскування.

Емуляція супротивника застосовується в критично важливих середовищах для стрес-тестування планів реагування на інциденти. Це дозволяє оцінити готовність організації до складних та цілеспрямованих атак.

Варто зазначити, що головною різницею між симуляцією загроз та емуляцією атаки полягає в тому, що емуляція атаки показує сильні та слабкі сторони атакуючих, використовуючи їх інструменти, в той час як симуляція загроз здебільшого фокусується на окремих частинах атаки та перевірки можливості реалізації конкретного сценарію [65]. Отже, симуляція загроз є базовою практикою для загального зміцнення безпеки, тоді як емуляція супротивника надає детальні уявлення про захист від складних, реальних атакуючих.

Розглянемо порівняння симуляції загроз та емуляції супротивника у вигляді таблиці:

Таблиця 2.1

Порівняння симуляції загроз та емуляції супротивника

Аспект	Симуляція загроз	Емуляція супротивника
Обсяг	Широкий спектр охоплення загальних загроз.	Орієнтований на конкретні TTP (тактики, техніки та процедури) атакуючих.
Джерело даних	Гіпотетичні сценарії атак, загальні шаблони атак.	Реальна розвідка про загрози (наприклад, MITRE ATT&CK, дані про APT-групи).
Автоматизація	Високий рівень автоматизації (використовуються BAS-платформи).	Рівень автоматизації варіюється залежно від критеріїв тестування .
Основна мета	Виявлення недоліків в системах захисту та оцінка ефективності безпекових заходів.	Перевірка здатності системи до виявлення та реагування на реальні атаки супротивника.
Час виконання	Виконується регулярно або постійно для моніторингу безпеки.	Може виконуватись періодично або за конкретними сценаріями атак.
Рівень деталізації	Виявлення загальних проблем безпеки та прогалин у захисті.	Глибокий аналіз конкретних загроз, виявлення недоліків у механізмах реагування.
Результати	Вузькі рекомендації щодо покращення безпеки та усунення недоліків що стосуються чітких прогалин в системах захисту.	Висновки про рівень захищеності від певних атак, ефективність механізмів виявлення та реагування.

продовження таблиці 2.1

Вартість	Відносно низька через високий рівень автоматизації.	Варіюється: у випадку автоматизації вартість знижується, але ручні тести з залученням Red Team залишаються дорогими.

2.4 Purple teaming як новий підхід до взаємодії команд з безпеки

Purple Teaming є інноваційним підходом до тестування та вдосконалення кібербезпеки організації, що поєднує найкращі практики Red Team (атакувальної команди) і Blue Team (захисної команди). Цей метод спрямований на створення безперервного циклу взаємодії між атакувальними та захисними групами для покращення виявлення загроз, оптимізації комунікації між командами та адаптації до реальних кіберзагроз [66].

Purple Teaming не є окремою командою – це скоріше методологія, яка забезпечує ефективну взаємодію між Red Team та Blue Team. Red Team імітує реальні кібератаки, що допомагає виявляти вразливості в інфраструктурі організації, тоді як Blue Team відповідає за захист, моніторинг і реагування на інциденти. Однак основною відмінністю Purple Teaming є постійна взаємодія цих двох груп, що дозволяє швидко коригувати стратегії захисту на основі реальних результатів атак.

Використання Purple Teaming дозволяє підвищити ефективність реагування на загрози шляхом оцінки виявлення атак, швидкості реакції на інциденти та ефективності існуючих захисних механізмів.

Системи симуляції кібератак є важливим інструментом у Purple Teaming. Вони дозволяють моделювати різноманітні кібератаки в умовах, максимально наближених до реальних, без ризику для операційної діяльності організації. BAS платформи, такі як Picus Security, SafeBreach або AttackIQ, автоматизують процес тестування і допомагають виявляти вразливості в системах захисту. Використання таких

інструментів дозволяє регулярно перевіряти ефективність захисту без необхідності постійної участі Red Team, що значно знижує витрати на ресурсах.

Ці платформи дозволяють тестувати захисні механізми за допомогою актуальних тактик, технік та процедур (TTPs), що застосовують реальні зловмисники, що дає змогу адаптувати стратегії захисту до нових загроз.

Взаємодія між Red Team і Blue Team у рамках Purple Teaming є ключовою для забезпечення ефективного процесу вдосконалення кіберзахисту [67]:

1. Red Team здійснює атаку, імітуючи дії реальних зловмисників. Це можуть бути фішингові атаки, експлуатація вразливостей у програмному забезпеченні, бічний рух у мережі або викрадення облікових даних.

2. Blue Team аналізує і реагує на ці атаки, застосовуючи наявні засоби захисту, такі як SIEM (Security Information and Event Management) або EDR (Endpoint Detection and Response).

3. Після завершення симуляції обидві команди обговорюють результати: чи була атака виявлена, як швидко відбулося реагування, чи існують уразливості, які потребують усунення.

4. На основі отриманих даних вносяться корективи в стратегію кіберзахисту, а також покращуються захисні механізми для забезпечення більшої стійкості до нових загроз.

Цей процес забезпечує не лише виявлення слабких місць у захисті, а й дозволяє оперативно адаптувати стратегії безпеки, створюючи тим самим більш динамічну та адаптивну систему захисту.

Розглянемо переваги використання purple team [68]:

1. Purple Teaming дозволяє глибше розуміти слабкі місця IT-інфраструктури завдяки постійному тестуванню і виявленню вразливостей.

2. Оскільки Red і Blue Team традиційно працюють окремо, між ними може виникати інформаційний розрив. Purple Teaming усуває цей розрив, забезпечуючи ефективну співпрацю та зворотний зв'язок.

3. Використання Purple Teaming дає можливість адаптувати стратегії захисту до актуальних загроз і атакувальних технік, що застосовують реальні кіберзлочинці та APT-групи.

4. Використання BAS-платформ дозволяє регулярно тестувати захист без залучення великих ресурсів, а також забезпечує безперервне вдосконалення кіберзахисту.

5. Завдяки інтеграції Red і Blue Team в один процес можна значно знизити витрати на кібербезпеку, при цьому отримуючи більш точні результати щодо стану захисту.

Purple Teaming є потужним інструментом для постійного вдосконалення кіберзахисту, який сприяє глибшому аналізу та виявленню вразливостей в системах захисту. Завдяки інтеграції Red і Blue Team, а також використанню BAS-платформ, організації можуть створити більш адаптивну та стійку до сучасних загроз кіберзахисну інфраструктуру.

Цей підхід дозволяє значно покращити ефективність роботи команд, а також забезпечити більш проактивну та результативну стратегію захисту, що є необхідною умовою для протидії постійно еволюціонуючим кіберзагрозам.

2.5 Порівняння традиційних методів тестування та систем симуляції кібератак

Для чіткого розуміння місця систем симуляції кібератак в загальній системі захисту організації, доцільно проаналізувати чіткі відмінності між всіма заходами, котрі спрямовані на виявлення недоліків в системах захисту. Будемо розглядати пентест, red teaming, аудити безпеки та BAS системи.

- **Мета кожного з заходів:**

Пентест фокусується на виявленні конкретних вразливостей шляхом моделювання реальних атак на системи та мережі. В той час як Red Teaming має більш комплексний характер, оцінюючи не лише технічні аспекти безпеки, а й здатність організації реагувати на загрози. Внутрішні аудити спрямовані на перевірку

відповідності політик і процедур внутрішнім стандартам та нормативним вимогам. BAS-системи автоматизують процес постійного тестування системи, виконуючи регулярне моделювання атак для виявлення вразливостей у режимі реального часу.

- **Процес тестування:**

Пентест проходить через етапи збору інформації, аналізу вразливостей, експлуатації, пост-експлуатації та підготовки звіту. Red Teaming передбачає використання сценаріїв реальних атак із залученням соціальної інженерії та перевіркою фізичної безпеки. Внутрішні аудити фокусуються на перевірці політик доступу, оцінці відповідності стандартам та аналізі логів. BAS-системи постійно виконують автоматизовані атаки на систему, перевіряючи надійність засобів захисту, та надають детальні звіти з рекомендаціями щодо усунення вразливостей.

- **Охоплення та глибина:**

Пентест зазвичай охоплює конкретні системи чи додатки, Red Teaming оцінює всю організаційну інфраструктуру, включаючи процеси реагування на атаки. Внутрішні аудити зосереджені на перевірці дотримання політик безпеки та відповідності стандартам. BAS-системи моделюють різноманітні сценарії атак, перевіряючи всю систему на стійкість до сучасних загроз.

- **Періодичність:**

Пентести та Red Teaming зазвичай проводяться 1–2 рази на рік, що може бути недостатнім для виявлення нових загроз. Внутрішні аудити відбуваються частіше, але здебільшого фокусуються на формальній перевірці політик. BAS-системи працюють у безперервному режимі, дозволяючи оперативно виявляти нові вразливості та реагувати на них у реальному часі.

- **Ресурси та вартість:**

Red Teaming вимагає значних ресурсів та залучення висококваліфікованих фахівців, що робить цей підхід дорогим. Пентест є менш витратним, оскільки фокусується лише на певних системах. Внутрішні аудити часто дешевші, оскільки виконуються власними силами організації. BAS-системи вимагають початкових

інвестицій у програмне забезпечення, але значно знижують витрати у довгостроковій перспективі завдяки автоматизації тестування.

Оптимальним є поєднання всіх підходів для забезпечення максимальної стійкості організації до кібератак. Пентест допомагає знайти технічні вразливості, Red Teaming забезпечує комплексне бачення безпеки, внутрішні аудити підтримують відповідність стандартам, а BAS-системи надають постійний моніторинг і оперативне виявлення нових загроз та недоліків в системах захисту.

Розглянемо основні відмінності між BAS, Red Teaming, пентестом та аудитами безпеки у вигляді таблиці [69, 70, 71]:

Таблиця 2.2

Порівняння BAS, Red teaming, пентест, аудити безпеки

Напрям	**BAS**	**Red Teaming**	**Пентест**	**Аудити безпеки**
Мета	Автоматизація перевірки безпеки шляхом симуляції кібератак для безперервного виявлення прогалин в безпеці.	Проведення реалістичної емуляції дій зловмисника для тестування загальної стійкості організації до загроз, включно з перевіркою здатності виявлення та реагування.	Виявлення технічних вразливостей шляхом симуляції цілеспрямованих атак на конкретні системи чи додатки.	Перевірка відповідності політик і процедур безпеки внутрішнім та зовнішнім стандартам, оцінка організаційних процесів.

продовження таблиці 2.2

Охоплення	Орієнтується на перевірку ефективності заходів безпеки та виявленні вразливостей.	Тестує заходи безпеки, реакцію людей та загальну стійкість організації.	Фокус на технічних аспектах безпеки конкретних систем або додатків.	Оцінка всієї системи безпеки з фокусом на відповідність нормативним вимогам.
Складність атак	Використовує заздалегідь визначені сценарії атак і тактики.	Імітує складні багатоступеневі атаки, адаптовані під унікальні профілі противника.	Орієнтується на експлуатацію відомих вразливостей та обхід захисту.	Не передбачає виконання реальних атак, зосереджуєтьс я на аналізі політик та процесів.
Налаштування	Переважно структурований і повторюваний підходу.	Повністю адаптується до середовища організації.	Налаштовується під конкретні системи та сценарії атаки.	Відповідно до стандартів безпеки, регламентів та політик.
Автоматизація	Високий рівень автоматизації, мінімізує потребу в людському втручанні.	Переважно ручний процес, що вимагає участі досвідчених фахівців з тестування на проникнення та етичних хакерів.	Частково автоматизований процес, з використанням спеціалізованих інструментів для виявлення вразливостей.	Переважно ручний процес, що включає перевірку документів, логів та налаштувань.

продовження таблиці 2.2

Емуляція загроз	Імітує поширені й новітні техніки атак на основі відомих даних про загрози.	Відтворює поведінку реальних загроз типу APT (Advanced Persistent Threat — розвинені постійні загрози).	Фокус на конкретних технічних векторах атак.	Не передбачає безпосередньо го моделювання атак.
Перевірка людського фактора	Орієнтуєтьс я на технічні заходи безпеки, здебільшого без оцінки реакції людей.	Активно перевіряє дії команд реагування на інциденти, аналітиків безпеки та процеси прийняття рішень керівництвом.	Мінімальна увага людському фактору, зосереджений на технічних аспектах.	Оцінює усвідомлення працівників щодо політик безпеки та процедур реагування.
Звітування та усунення вразливост ей	Генерує автоматизов ані звіти з виявленням прогалин у захисті та рекомендац іями щодо їх усунення.	Створює детальні звіти з якісним аналізом, спостереженнями про дії зловмисників та стратегіями пом’якшення наслідків.	Надає звіт про знайдені технічні вразливості та рекомендації щодо їх усунення.	Формує звіт про відповідність, виявлені невідповіднос ті та рекомендації для покращення.

продовження таблиці 2.2

Частота використання	Можна налаштувати бажану частоту виконання симуляцій, наприклад щоденно.	Зазвичай проводиться 1–2 рази на рік.	Залежить від потреб організації, зазвичай 1–2 рази на рік.	Проводиться регулярно (щоквартально, щорічно) або в рамках аудиторських перевірок.
Ціна	Дешевший процес за рахунок автоматизації.	Дорожчий процес за рахунок виконання ручної роботи.	Помірна вартість, залежить від обсягу тестування та складності системи.	Менша вартість, особливо якщо виконується внутрішніми силами.

Системи моделювання атак та порушень (BAS) є потужним інструментом для автоматизованої оцінки кібербезпеки організації. Вони дозволяють регулярно та безперервно симулювати кібератаки, виявляючи вразливості та перевіряючи ефективність існуючих заходів захисту. Однак, попри їхню ефективність, BAS не можуть повністю замінити такі методи, як Red Teaming, пентестинг та аудити безпеки.

Red Teaming передбачає комплексну імітацію дій реальних зловмисників, включаючи використання соціальної інженерії, фізичного доступу та інших нестандартних методів атак. Цей підхід дозволяє оцінити не лише технічні аспекти безпеки, але й готовність персоналу до реагування на інциденти. BAS-системи, будучи автоматизованими, не можуть повністю відтворити такі складні та непередбачувані сценарії, які характерні для Red Teaming.

Пентестинг, або тестування на проникнення, фокусується на виявленні конкретних вразливостей у системах та додатках шляхом активного пошуку та експлуатації цих вразливостей. Хоча BAS може автоматично виявляти відомі вразливості, вони не завжди здатні ідентифікувати нові або специфічні для конкретної організації слабкі місця, які можуть бути виявлені під час ручного пентесту.

Аудити безпеки зазвичай включають всебічний аналіз політик, процедур та відповідності нормативним вимогам. Цей процес передбачає глибоке розуміння бізнес-процесів, культури компанії та специфічних ризиків, що виходить за межі технічних можливостей BAS.

Отже, хоча BAS-системи є важливим компонентом стратегії кібербезпеки, вони не можуть повністю замінити Red Teaming, пентестинг та аудити безпеки. Найбільш ефективний підхід до забезпечення безпеки полягає у поєднанні автоматизованих інструментів, таких як BAS, з ручними методами оцінки, що дозволяє отримати комплексне розуміння стану безпеки організації та забезпечити її стійкість до різноманітних загроз [72].

Висновки до другого розділу

У розділі було розглянуто сучасні підходи до перевірки ефективності засобів кіберзахисту, зокрема симуляцію кібератак. Особливу увагу приділено системам класу BAS, які дозволяють автоматизовано відтворювати сценарії атак у контрольованому середовищі.

BAS-рішення надають можливість регулярно перевіряти готовність систем безпеки до типових технік зловмисників, орієнтуючись на базу знань MITRE ATT&CK. У порівнянні з цим, Red Teaming передбачає глибоке моделювання поведінки реального супротивника, охоплюючи також соціальну інженерію, фізичний доступ і нестандартні методи обходу захисту. Red Team-операції вимагають більше часу, ресурсів і проводяться рідше, але дають більш комплексну картину реальних ризиків. Пентестинг, на відміну від Red Teaming, має чітко визначені межі та зосереджується переважно на виявленні конкретних технічних вразливостей.

Аудити безпеки є ще більш формалізованими, спрямованими на перевірку відповідності політикам, стандартам або вимогам. Важливо підкреслити, що жоден із підходів не є універсальним — кожен має своє призначення та доповнює інші.

BAS-тестування є ефективним інструментом постійного моніторингу і дозволяє підтримувати високий рівень обізнаності про актуальний стан захисту. Дані з BAS-платформ можуть використовуватись для оперативного виявлення змін у поведінці систем безпеки між більш рідкісними, але глибокими перевірками. При цьому, симуляція та емуляція кібератак мають різні цілі: перша зосереджена на типових шаблонних атаках, друга — на конкретній моделі поведінки певного типу загрози. Поєднання методів тестування дозволяє організації перейти від реактивного до проактивного підходу в кіберзахисті.

Загалом, розглянуті методи відіграють важливу роль у вдосконаленні процесів оцінки ризиків і прийняття рішень у сфері інформаційної безпеки. Їх комплексне використання дозволяє вчасно виявляти вразливості, перевіряти готовність до інцидентів і підвищувати загальний рівень кіберзахисту організації.

РОЗДІЛ 3
ТЕСТУВАННЯ СИСТЕМ ЗАХИСТУ З ВИКОРИСТАННЯМ СИСТЕМ СИМУЛЯЦІЇ КІБЕРАТАК

3.1 Інструменти для автоматизованого тестування захищеності

Існує кілька популярних рішень для симуляції дій зловмисників, кожне з яких має свої функціональні можливості. Розглянемо кожне з них детальніше:

- **MITRE Caldera [73]**

MITRE Caldera — це фреймворк для автоматизації дій атакуючих, розроблений на основі бази знань MITRE ATT&CK. Він дозволяє проводити як автономні симуляції вторгнень, так і підтримувати ручні операції червоних команд. Основні компоненти Caldera включають асинхронний сервер командування та контролю (C2) з REST API та веб-інтерфейсом. Фреймворк забезпечує автоматизоване тестування кіберзахисту, включаючи мережевий захист, захист кінцевих точок, журнали, аналітику та оповіщення, а також автоматизовану відповідь на інциденти. Крім того, Caldera підтримує розширення за допомогою плагінів, що додають додаткові можливості, такі як агенти, звітність та набори TTPs.

- **Atomic Red Team [74]**

Atomic Red Team — це відкрита бібліотека тестових сценаріїв, розроблена для перевірки захищеності систем. Кожен тест відповідає певній техніці з матриці MITRE ATT&CK. Ці тести можуть бути використані для перевірки ефективності заходів безпеки, тестування покриття виявлення та навчання розпізнаванню шкідливої активності. Для спрощення виконання тестів розроблено фреймворк Invoke-Atomic, який автоматизує процес запуску окремих тестів або їхніх груп.

- **Picus Security [75]**

Платформа Picus пропонує комплексну перевірку захисту організацій від кібератак та дозволяє оцінити та оптимізувати ефективність безпекових контролів за допомогою симуляції атак. Picus допомагає виявляти шляхи атак, які можуть

використовувати зловмисники для компрометації користувачів та активів, забезпечує перевірку правил виявлення, щоб оптимізувати їхню ефективність і виявити потенційні проблеми у їхньому функціонуванні. Також аналізує конфігурації хмарних середовищ та політики керування доступом для запобігання надмірним дозволам і неправильним налаштуванням. Picus підтримує постійну валідацію безпекової інфраструктури, включаючи інтеграцію з рішеннями безпеки, що дозволяє організаціям перевіряти коректність налаштування систем захисту перед потенційними атаками. Платформа також включає детальні звіти про виявлені недоліки та пропонує кроки для їх усунення.

- **Cymulate [76]**

Cymulate пропонує комплексну платформу для перевірки кібербезпеки, яка допомагає організаціям оцінювати свою стійкість до загроз. Вона використовує моделювання атак для імітації реальних кібератак та виявлення прогалин у захисті. Платформа дозволяє тестувати ефективність засобів безпеки на всіх етапах атаки — від проникнення до розповсюдження та дій зловмисників. Cymulate також оцінює ефективність виявлення загроз та реакції на інциденти, щоб покращити процеси реагування. Завдяки автоматизації тестування, організації можуть постійно відстежувати рівень своєї кіберстійкості в режимі реального часу. Платформа надає детальні звіти та рекомендації для усунення вразливостей, що дозволяє швидко зміцнити захист. Cymulate підтримує інтеграцію з іншими системами безпеки, спрощуючи процеси моніторингу та покращення захисту.

- **Pentera [77]**

Pentera пропонує автоматизовану платформу для перевірки кібербезпеки шляхом симуляції реальних атак. Вона дозволяє організаціям оцінювати стійкість своїх систем, імітуючи дії зловмисників у контрольованому середовищі. Платформа виявляє прогалини в безпеці на всіх етапах потенційної атаки — від проникнення до руху в мережі організації. Pentera аналізує захисні механізми та надає рекомендації для усунення недоліків у безпеці. Завдяки автоматизації процесу, організації можуть проводити регулярні перевірки безпеки без необхідності в ручних тестах. Платформа генерує детальні звіти з описом знайдених ризиків і пропонує практичні кроки для

їхнього усунення. Pentera допомагає підвищити кіберстійкість, дозволяючи виявляти й закривати прогалини до того, як ними скористаються зловмисники.

3.2 Визначення недоліків в системах захисту

СК може виявити наступні недоліки в системах захисту:

- **Відсутність або слабкі механізми виявлення атак** – якщо система не фіксує або погано розпізнає атаки, це може вказувати на проблеми з SIEM, EDR, IDS/IPS або іншими засобами захисту.
- **Неправильне управління правами доступу** – надмірні привілеї користувачів або службових акаунтів можуть дозволити атакуючому швидко отримати контроль над системою, в той час як СЗ можуть бути відключені привілейованим користувачем.
- **Недостатня ізоляція критичних систем** – відсутність сегментації мережі або слабкий контроль трафіку можуть дозволити атакуючим поширюватися всередині організації.
- **Вразливі або застарілі програмні компоненти** – наявність відомих вразливостей у програмному забезпеченні або відсутність оновлень може створювати точки входу для атак.
- **Недостатній захист від фішингових атак** – якщо симуляція атак виявляє високу ймовірність успішного фішингу серед персоналу, це свідчить про недостатні заходи контролю доступу.
- **Слабке логування та відстеження активності** – відсутність детального журналювання або його неправильна конфігурація можуть ускладнювати розслідування атак і вчасне реагування.
- **Повільне або неефективне реагування на інциденти** – якщо система безпеки або персонал не можуть швидко і правильно відреагувати на атаку, це може вказувати на відсутність плану реагування або недостатню підготовку команди SOC.

• **Занадто широкі виключення в системах захисту** – при виникненні false positive частою практикою є внесення виключень для певних папок чи файлів в системах захисту. Іноді такі виключення можуть бути занадто широкими, дозволяючи виконання не лише легітимних файлів, а й відкриваючи можливість зловмисникам для реалізації атак.

3.3 Інтеграція систем симуляції атак з існуючими системами кібербезпеки

Щоб симуляція атак була максимально ефективною, вона має зручно вбудовуватися в екосистему захисних рішень організації. Така інтеграція дозволяє не лише краще виявляти недоліки систем захисту, а й покращувати механізми реагування, оптимізувати процеси моніторингу та зміцнювати загальну кіберстійкість.

Одним із ключових напрямів інтеграції є взаємодія з SIEM-системами, які відповідають за збір та аналіз подій із різних джерел. Поєднання симуляції атак із SIEM дозволяє перевірити, наскільки швидко система здатна зафіксувати підозрілу активність, як ефективно налаштовані кореляційні правила та чи достатньо інформативними є сповіщення. У процесі тестування виявляються прогалини у виявленні, що дає змогу вдосконалювати політики безпеки на основі реальних сценаріїв атак.

Не менш важливою є інтеграція з EDR-рішеннями, які забезпечують захист кінцевих точок та реагування на шкідливі дії. У такій комбінації симуляція дозволяє перевірити, наскільки швидко система виявляє спроби компрометації та чи ефективно блокує підозрілу активність. Крім того, отримані результати можна використовувати для налаштування автоматичних реакцій на загрози, підвищуючи рівень захисту без участі людини.

Дані, отримані внаслідок симуляцій, мають велике значення для оновлення політик безпеки. На їх основі можна актуалізувати правила моніторингу, покращити алгоритми реагування та налаштувати більш точні механізми виявлення загроз. Це

дозволяє організації не лише реагувати на виявлені недоліки, а й створювати проактивні механізми захисту.

Автоматизація процесів реагування відіграє важливу роль у зменшенні часу між виявленням інциденту та його нейтралізацією. Інтеграція симуляцій із SOAR-платформами дозволяє автоматично запускати сценарії реагування, корелювати дії різних захисних систем і створювати інциденти у журналах безпеки. Це не лише пришвидшує процес реагування, а й знижує ймовірність людської помилки під час критичних ситуацій.

Для наочного прикладу можна розглянути розробку моделі тестування корпоративних систем. Зокрема, сценарій перевірки ефективності роботи SIEM/EDR може передбачати імітацію спроби бічного руху всередині мережі. У процесі такого тестування оцінюється, як швидко система виявить ці дії та чи зможе правильно класифікувати загрозу. Інший приклад — моделювання атаки на корпоративну пошту, що дозволяє перевірити реакцію системи на підроблені листи, вкладення зі шкідливим кодом чи спроби компрометації облікових записів.

Таким чином, інтеграція систем симуляції атак із захисною інфраструктурою дозволяє створити цілісну картину стійкості організації до сучасних кіберзагроз. Вона сприяє не лише покращенню механізмів захисту, а й вдосконаленню процесів автоматичного реагування, підвищенню обізнаності персоналу та забезпеченню безперервного покращення рівня безпеки.

3.4 Етапи методу тестування систем захисту з використанням симуляції кібератак

Серед етапів, які включає метод тестування СЗ з використанням СК, можна виділити наступні [78]:

- Ідентифікація цілей симуляції, визначення загроз і вибір тактик атак.
- Вибір інструментів для реалізації атак.
- Розгортання та налаштування системи симуляції кібератак.

- Налаштування інтеграцій між системою симуляції кібератак та системами захисту.
- Формування сценаріїв атак.
- Впровадження та тестування сценаріїв.
- Аналіз отриманих результатів.
- Визначення недоліків в системах захисту.
- Усунення недоліків в системах захисту.
- Проведення повторного тестування.

Процес тестування систем захисту з використанням симуляції кібератак починається з визначення цілей симуляції, виявлення потенційних загроз і вибору відповідних тактик атак.

Далі здійснюється підбір інструментів, які дозволять ефективно реалізувати ці атаки у контрольованому середовищі.

Наступним кроком є розгортання та налаштування системи симуляції, що включає забезпечення її готовності до виконання сценаріїв.

Після цього налаштовуються інтеграції між системою симуляції та засобами захисту, якщо такі наявні, для забезпечення повного збору даних. Формуються сценарії атак, що відображають реалістичні моделі поведінки зловмисників, та виконується їх впровадження і тестування.

На основі результатів тестування проводиться аналіз, який дозволяє виявити недоліки в наявних засобах захисту.

Завершальним етапом є усунення цих недоліків та проведення повторного тестування для перевірки ефективності внесених змін.

Розглянемо етапи методу у вигляді блок схеми (Рис. 3.1):

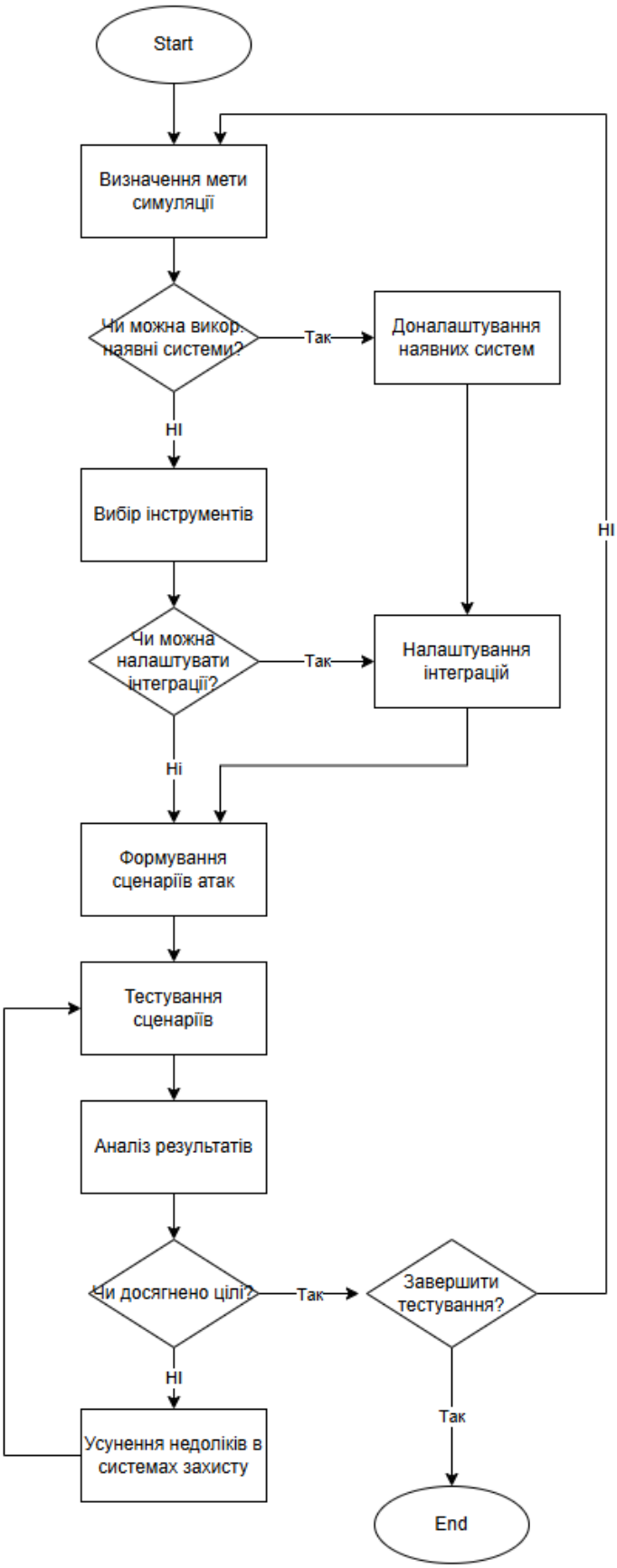

Рисунок 3.1 – Загальна блок-схема методу тестування систем захисту з використанням симуляції кібератак

Для правильного вибору системи симуляції кібератак, організаціям потрібно враховувати кроки, що дозволяють коректно визначити, яке саме рішення потрібне для їх випадку, а також як в подальшому використовувати його для отримання максимальних переваг.

Першочерговим завданням є чітке визначення цілей симуляції. Це може бути перевірка здатності системи виявляти певні типи атак, оцінка часу реагування або виявлення слабких місць у захисті. Для структурованого аналізу загроз доцільно використовувати такі фреймворки як MITRE ATT&CK чи Cyber Kill Chain, що дозволяють розділити атаку на етапи та краще зрозуміти поведінку потенційних зловмисників. На цьому етапі також важливо врахувати типові загрози для конкретного середовища, зокрема фішинг, експлуатацію вразливостей або рух зловмисника мережею після проникнення.

Наступний крок передбачає аналіз доступних інструментів для симуляції. Вибір залежить від цілей тестування, складності інфраструктури та потреб організації. Деякі рішення фокусуються на автоматизації процесів (BAS), інші більше підходять для ручного тестування або емуляції конкретних тактик зловмисників (наприклад, використання Cobalt Strike чи Metasploit). Важливим аспектом є не лише функціональність інструменту, а й його здатність інтегруватися з наявними системами захисту, такими як SIEM чи EDR. Ще один надзвичайно важливий аспект, який важливо враховувати – постійне поповнення системи новими загрозами для розширення обсягу ТС захисту та можливості симулювати актуальні загрози, які потенційно можуть загрожувати організації на даний момент.

Не менш важливим етапом є розгортання та зручність експлуатації систем симуляції кібератак. Важливо щоб система надавала коректну інформацію щодо необхідних виключень в системах захисту для її роботи, легко встановлювалась та масштабувалась. Зручний інтерфейс користувача дозволить адміністраторам системи якнайшвидше дослідити функціонал та легко використовувати систему в щоденній роботі.

Після розгортання інструментів необхідно розробити детальні сценарії атак, що імітують реальні дії зловмисників. Це включає визначення початкових точок

проникнення, методів закріплення у системі, технік приховування слідів та способів ексфільтрації даних. Якісні сценарії повинні охоплювати не лише очікувані загрози, а й малоймовірні сценарії, що дозволяють оцінити стійкість системи до нетипових атак.

На етапі впровадження та тестування сценаріїв реалізуються підготовлені сценарії у контрольованому середовищі або безпосередньо в робочій інфраструктурі (якщо це дозволено політиками безпеки). Під час тестування відстежується, як система реагує на кожен етап атаки: чи спрацьовують механізми виявлення, чи створюються сповіщення в SIEM, як діють засоби захисту кінцевих точок (EDR) та наскільки швидко відбувається реагування. Це дозволяє отримати практичні дані про ефективність захисних механізмів та їхню здатність протидіяти сучасним загрозам.

Наступний етап полягає в детальному аналізі зібраних даних. Основна увага приділяється виявленим слабким місцям у системі безпеки, оцінці часу виявлення та реагування, а також точності спрацьовування існуючих механізмів захисту. На основі отриманих результатів формуються рекомендації щодо покращення політик безпеки, налаштувань захисних інструментів та впровадження додаткових заходів для зменшення ризиків у майбутньому.

В подальшому проводиться повторне тестування, яке дає змогу оцінити, чи були успішно впроваджені рекомендації з попередніх тестів, а також виявити нові недоліки, що могли з’явитися внаслідок змін у системі чи оновлення її компонентів. Крім того, СЗ постійно оновлюються відповідно до нових загроз, тому регулярне тестування дозволяє перевірити їхню актуальність і вчасно виявити ситуації, коли якийсь елемент захисту став менш ефективним або зовсім перестав працювати.

Висновки до третього розділу

У даному розділі розроблено метод тестування систем захисту з використанням автоматизованої симуляції кібератак. Описано етапи тестування систем захисту, які включають ідентифікацію цілей симуляції, визначення загроз і вибір тактик атак, вибір інструментів для реалізації атак, розгортання та налаштування системи

симуляції кібератак, налаштування інтеграцій між системою симуляції кібератак та системами захисту, формування сценаріїв атак, впровадження та тестування сценаріїв, аналіз отриманих результатів, визначення недоліків в системах захисту, усунення недоліків в системах захисту та проведення повторного тестування.

Симуляція кібератак є важливим інструментом для перевірки систем захисту та підвищення кіберстійкості організацій. Вона дозволяє виявляти слабкі місця в інфраструктурі шляхом відтворення реальних сценаріїв атак у контрольованих умовах. Інтеграція симуляцій із SIEM, EDR та SOAR системами забезпечує своєчасне виявлення загроз і автоматизацію процесів реагування. Це сприяє зниженню часу між виявленням інциденту та його нейтралізацією, що підвищує загальну стійкість системи.

Важливим етапом є правильний вибір інструментів для симуляції, що мають відповідати потребам організації та інтегруватися з наявними засобами захисту. Формування сценаріїв атак базується на реальних тактиках зловмисників, що дозволяє оцінити реакцію системи на різні методи проникнення й закріплення в мережі. Тестування таких сценаріїв у реальному середовищі виявляє як технічні, так і організаційні недоліки захисту.

Аналіз результатів симуляцій дозволяє не лише визначити слабкі місця, але й надати рекомендації щодо вдосконалення захисту. Повторне тестування після впровадження змін дає змогу оцінити їхню ефективність і контролювати актуальність захисних механізмів у динамічному середовищі загроз.

Регулярне проведення симуляцій забезпечує постійний моніторинг стану захисту, що дозволяє своєчасно виявляти та усувати нові уразливості.

Таким чином, симуляція кібератак є не лише інструментом виявлення недоліків, але й засобом для постійного вдосконалення кіберзахисту, що є критично важливим для сучасних організацій у контексті зростаючих загроз.

РОЗДІЛ 4
ПРАКТИЧНА ПЕРЕВІРКА МЕТОДУ ТЕСТУВАННЯ СИСТЕМ ЗАХИСТУ З ВИКОРИСТАННЯМ АВТМАТИЗОВАНОЇ СИМУЛЯЦІЇ КІБЕРАТАК

4.1 Використання інструменту AtomicRedTeam для перевірки коректності налаштування EDR системи

Для початку визначимо ціль симуляції, в даному випадку це буде перевірка захисту кінцевої точки від реалізації тактик потенційного зловмисника, що полягають в ескалації привілеїв (Privilege Escalation) та доступу до облікових даних (Credential Access). Варто зазначити, що викрадення облікових даних мало стосунок до 86% зламів [79], котрі відбуваються в організаціях, що повністю підтверджує актуальність подібного тестування. Щодо ескалації привілеїв – це теж надзвичайно розповсюджена практика серед зловмисників, оскільки дуже часто адміністративні облікові записи мають дуже широкі права та дозволяють виконувати в системі майже будь які дії.

Не усі організації мають змогу виділяти кошти на дороговартісну систему, котра дозволить повноцінно протестувати СЗ. Однак у відкритому доступі є фреймворки для проведення симуляцій кібератак, котрі дозволяють на базовому рівні здійснити перевірку наявних систем захисту. Для даного тестування було прийнято рішення використати фреймворк AtomicRedTeam.

Дане рішення можна встановити локально як модуль Powershell, використовуючи документацію [80], що й було виконано. Також можна переглянути загальний список тестів (Рис. 4.1), котрі дозволяє провести дане рішення. Кожний тест пов’язаний з відповідною тактикою та технікою з матриці MITRE, що дозволяє швидко визначити потрібний набір тестів для кожної задачі.

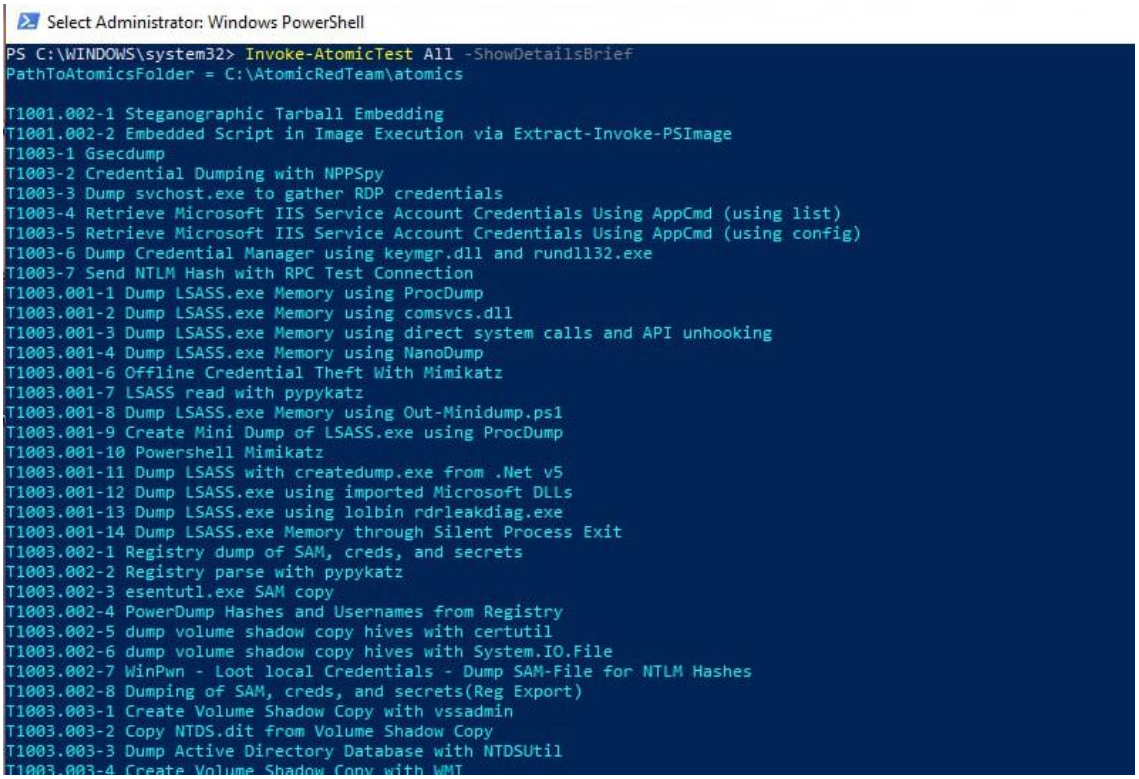

Рисунок 4.1 – Список доступних тестів AtomicRedTeam

Після чого можна детально розглянути кожний з тестів, переглянути опис його дій, чи задовольняються передумови для тестування та у випадку відсутності – встановити їх (Рис. 4.2).

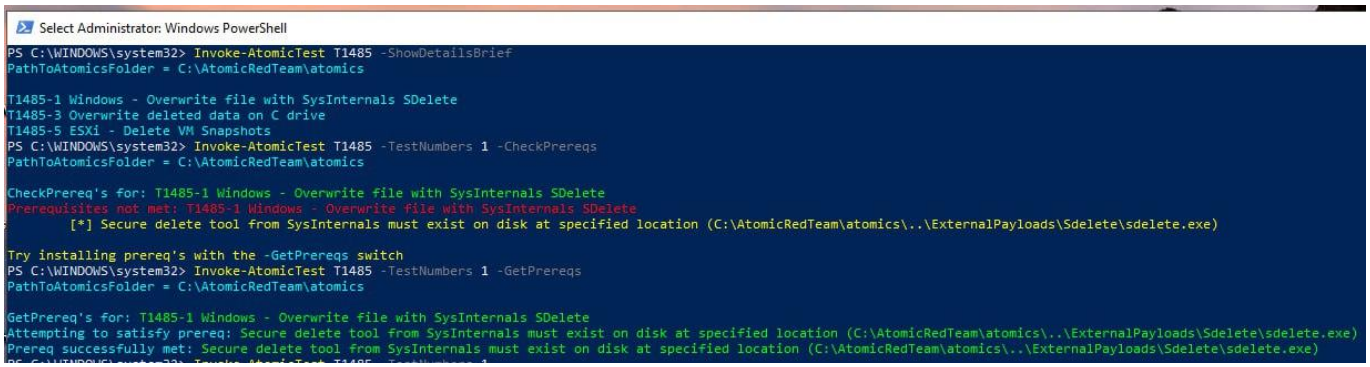

Рисунок 4.2 – Перевірка передумов та встановлення компонентів для можливості запуску тесту

Коли всі умови виконані, можна запустити окремий тест та перевірити готовність системи до більш масштабного застосування (Рис. 4.3).

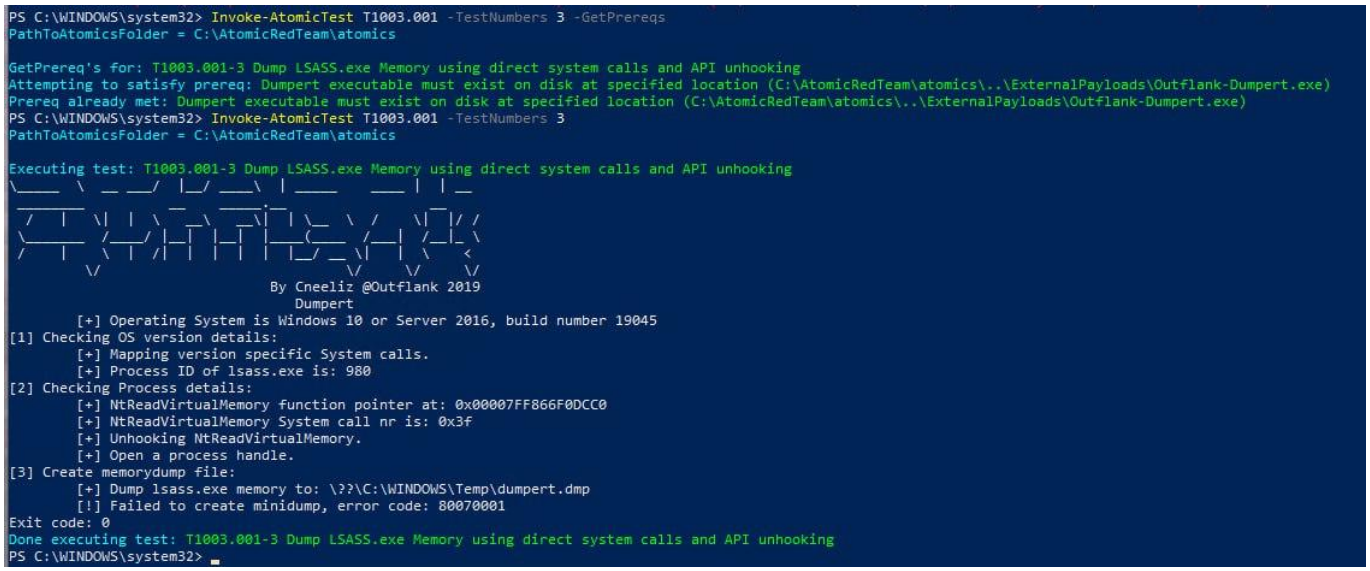

Рисунок 4.3 – Запуск тесту з симуляцією дій зловмисника

Переглянувши відповідну директорію, можна впевнитись, що дамп процесу lssass було успішно створено зловмисником (рис. 4.4), що означає коректність розгортання системи та готовність симулювати реальні дії зловмисника.

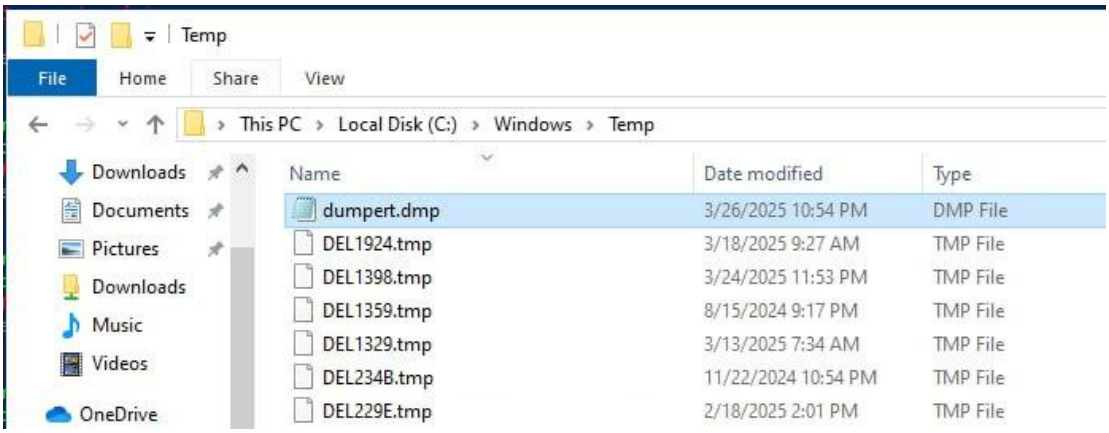

Рисунок 4.4 – Результат виконання симуляції дій зловмисника

Оскільки симуляції атак мають безпосередній вплив на систему, розкриваючи конфіденційні дані шляхом створення файлів з ними або вносячи перешкоди в коректне функціонування системи, важливо після кожного тестування виконувати очистку внесених симуляцією дій, щоб система повернулась до початкового стану (рис. 4.5).

```
PS C:\WINDOWS\system32> Invoke-AtomicTest T1003.001 -TestNumbers 3 -Cleanup
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing cleanup for test: T1003.001-3 Dump LSASS.exe Memory using direct system calls and API unhooking
Done executing cleanup for test: T1003.001-3 Dump LSASS.exe Memory using direct system calls and API unhooking
PS C:\WINDOWS\system32>
```

Рисунок 4.5 – Виконання команд для очищення змін в системі

Для формування сценаріїв атак, потрібно розглянути покриття матриці MITRE даним рішенням, для цього можна скористатись наявним у відкритому доступі списком тестів та функціоналом веб-ресурсу MITRE. Чим червоніший колір, тим більшу частину відповідних технік покриває рішення (рис. 4.6).

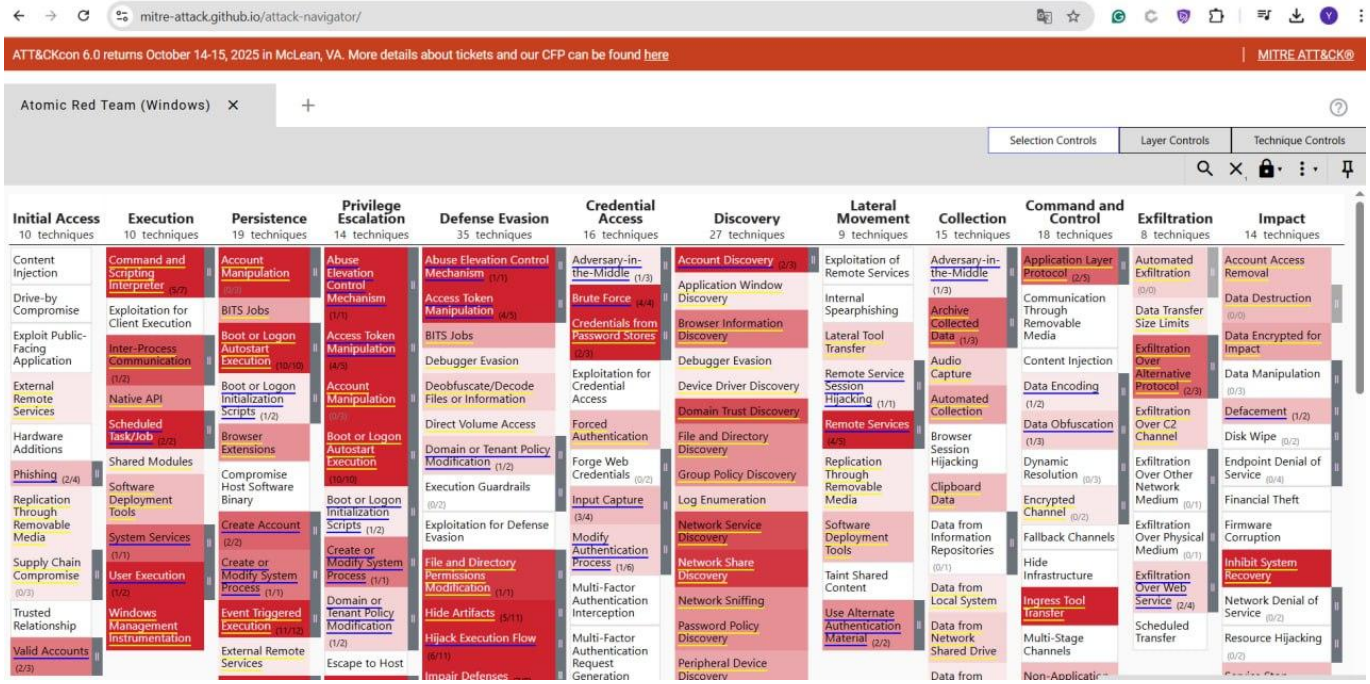

Рисунок 4.6 – Доступні для симуляції тести, відповідно до матриці MITRE.

Ознайомившись з доступними тестами, було прийнято рішення сформувати набір тестів, що включає наступні сценарії, їх опис можна переглянути в додатку Б:

- T1003.001
- T1003.002
- T1003.003
- T1053.005
- T1078.003
- T1134.004

- T1543.003
- T1546.008
- T1547.001
- T1547.004
- T1548.002
- T1552.001
- T1552.004
- T1555.003
- T1558.003

Після чого була запущена симуляція відповідно до створеного набору тестів (рис. 4.7).

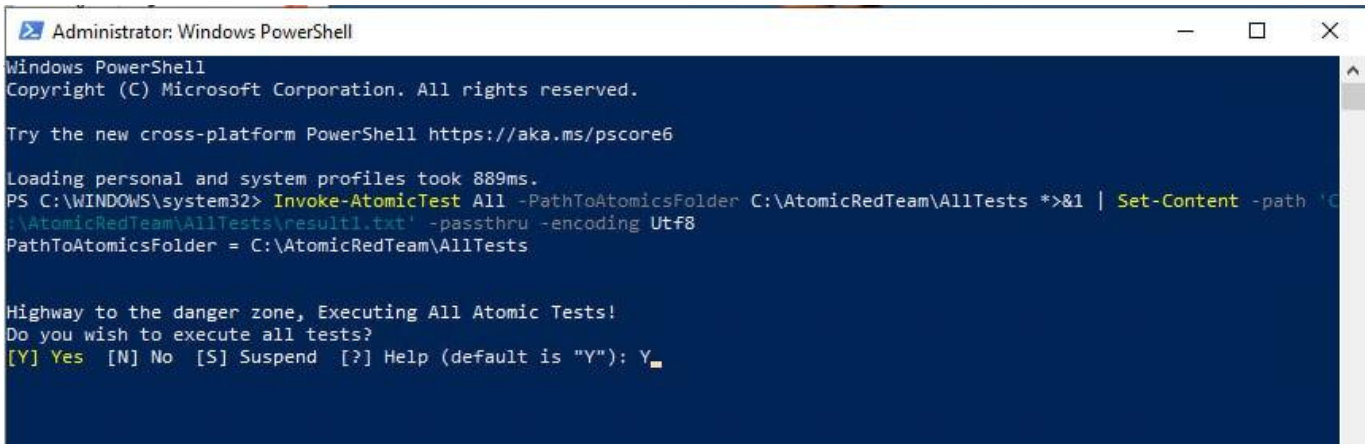

Рисунок 4.7 – Запуск симуляції для перевірки функціонування систем захисту

В процесі симуляції кібератаки, результати дій виводяться в консоль, тому можна зрозуміти чи успішною була зловмисна дія і чи вдалось системі захисту її заблокувати. Для прикладу можна розглянути атаку з техніки T1555.003 яка могла б призвезти до отримання потенційним зловмисником доступу до облікових даних користувачів (рис. 4.8).

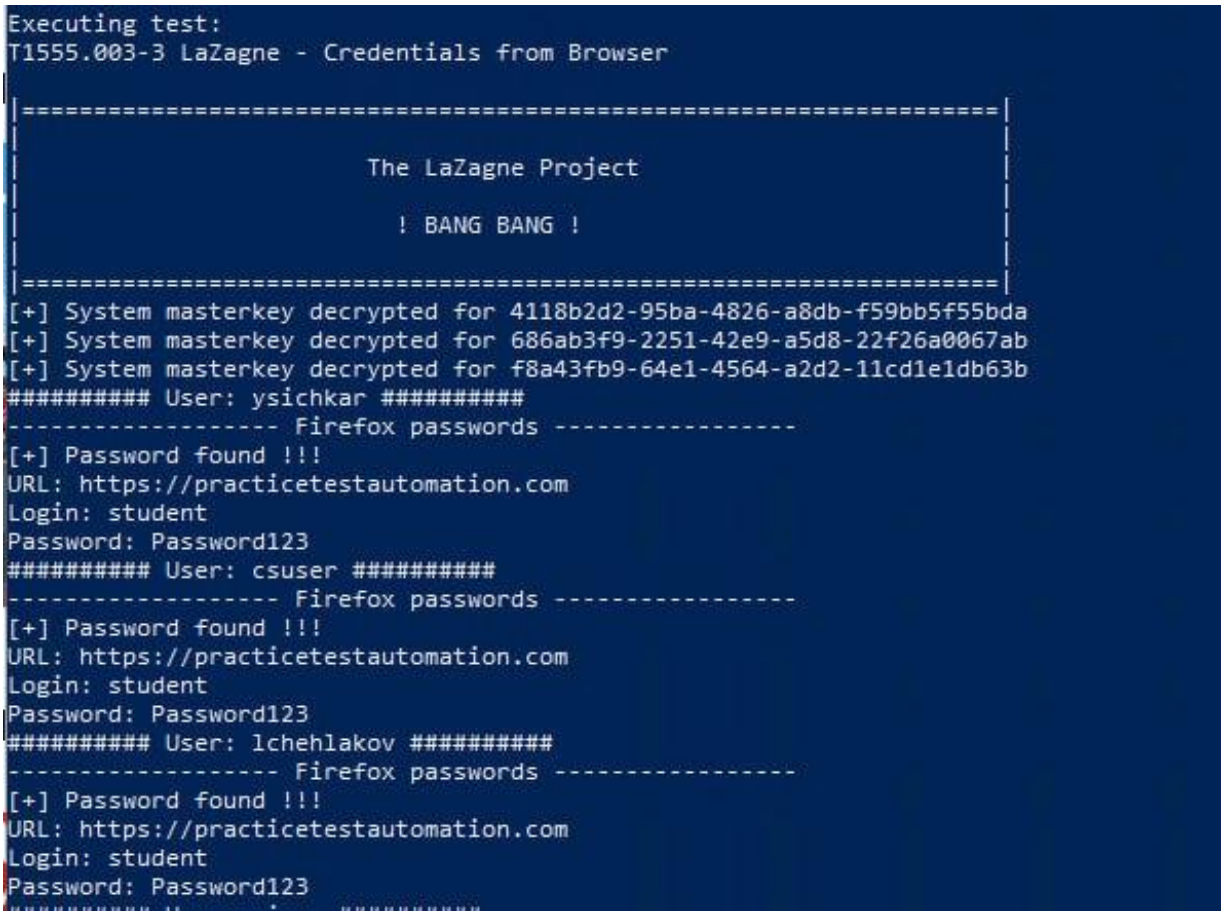

Рисунок 4.8 – Успішно виконана зловмисна дія, що призвела до компроментації облікових даних користувачів

Після завершення симуляції атаки, переходимо до аналізу результатів в системі захисту. В даному тестуванні системою захисту виступає CrowdStrike Falcon – лідер в напрямку захисту кінцевих точок [81]. Як можна побачити – система захисту сповіщає про 279 подій, які можуть свідчити про атаку. Причому серед усіх тактик, найбільшу частину даних сповіщень складає виконання скриптів, спроби доступу до облікових даних та ескалація привілеїв – саме ті дії які в основному виконувались під час симуляції (рис. 4.9).

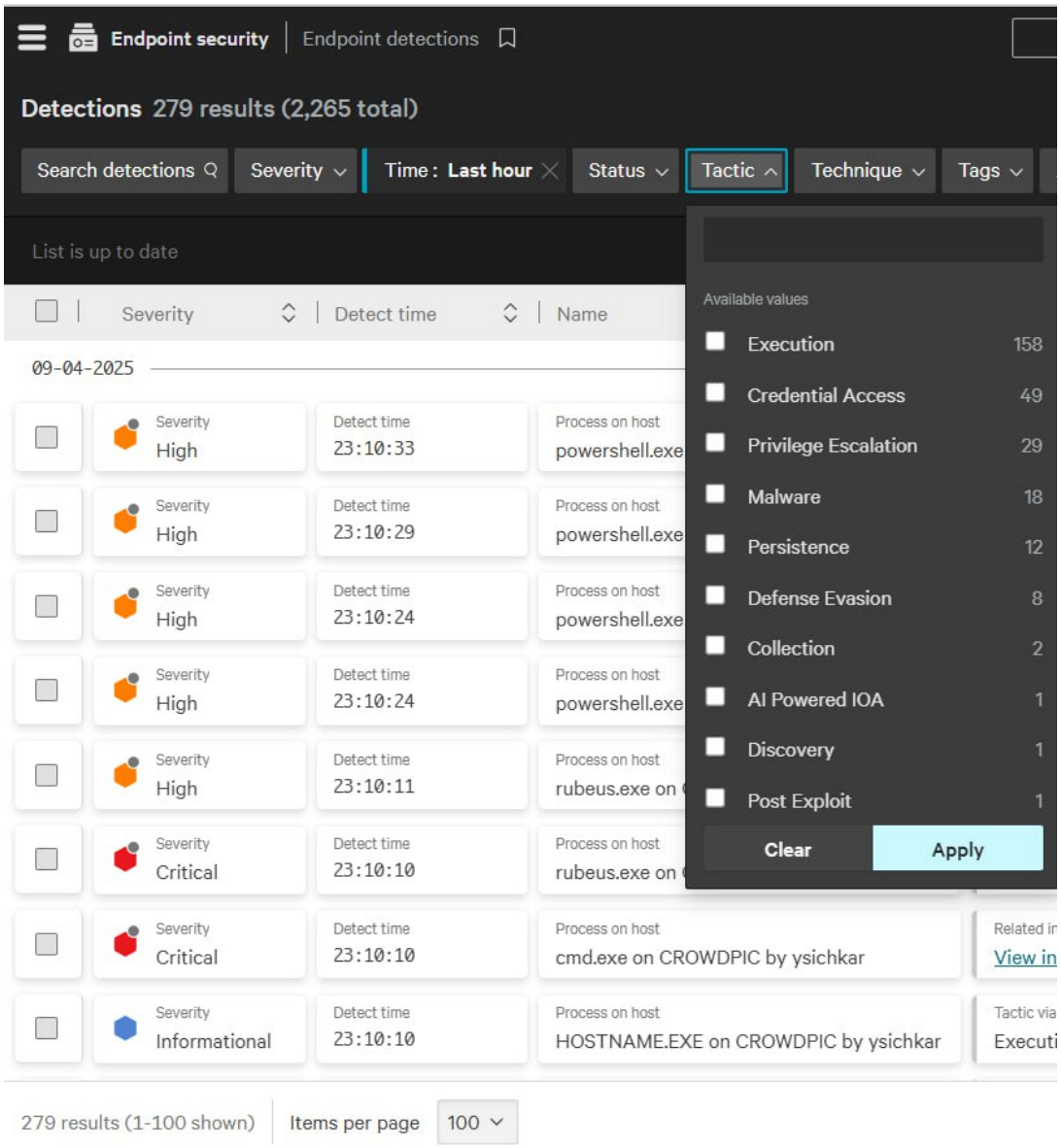

Рисунок 4.9 – Результати симуляції в системі CrowdStrike Falcon

Подальше дослідження може включати більш детальний розгляд кожного з спрацювань СЗ. Особливу увагу варто звернути на дію, що була застосована у відповідь на підозрілу активність. В обох випадках, на рисунку 4.10 та рисунку 4.11, система захисту не виконала ніяких дій для захисту кінцевого пристрою, хоча успішно було визначено навіть техніку даних атак. Цікавою деталлю на рисунку 11 є повідомлення СЗ, що блокування не відбулось, оскільки потрібний параметр в політиці захисту, яка застосовувалась до кінцевого пристрою, була вимкнена.

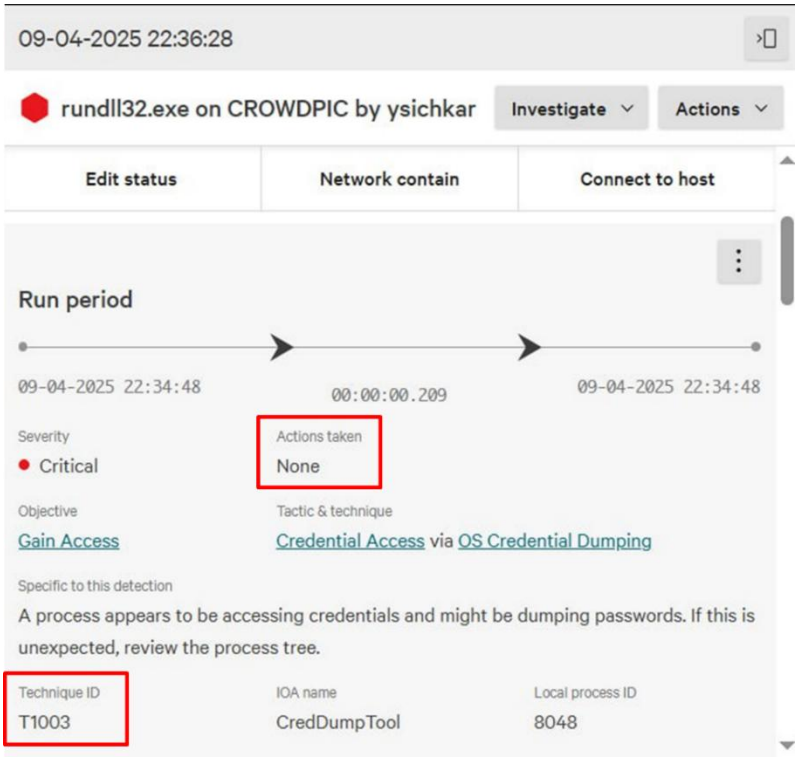

Рисунок 4.10 – Незаблокована активність, що стосувалась техніки T1003

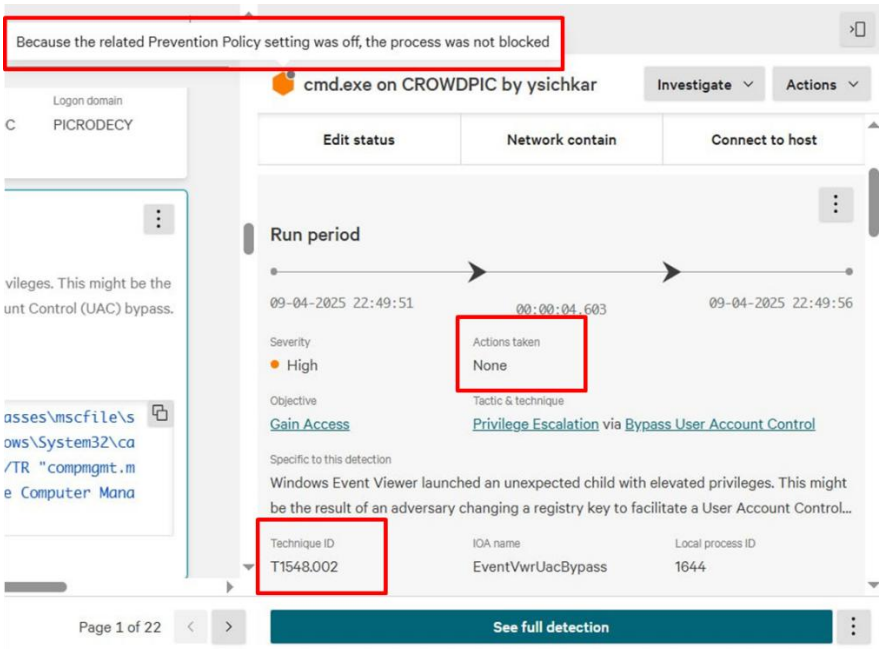

Рисунок 4.11 – Незаблокована активність, що стосувалась техніки T1548.002

Провівши дослідження політики захисту, котра використовується на даний момент, було виявлено, що деякі опції було вимкнено або до кінцевого пристрою було

застосовано тестову політику (рис. 4.12-4.14). Як результат – група хостів, котра мала цю саму політику, могла стали легкою ціллю хакерів.

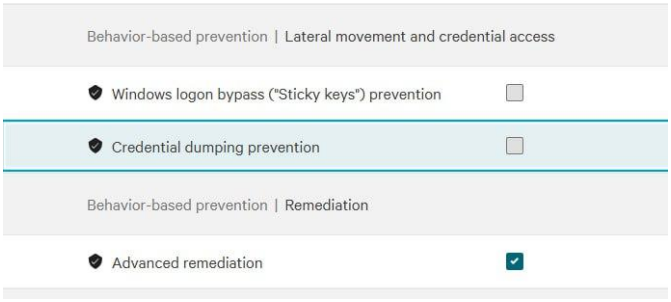

Рисунок 4.12 – Вимкнені опції в політиці захисту (ч.1)

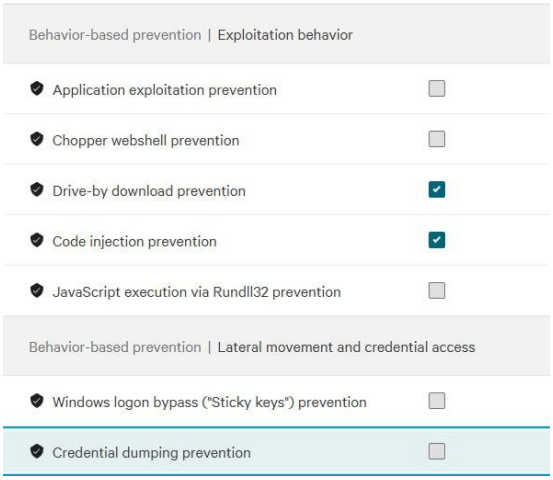

Рисунок 4.13 – Вимкнені опції в політиці захисту (ч.2)

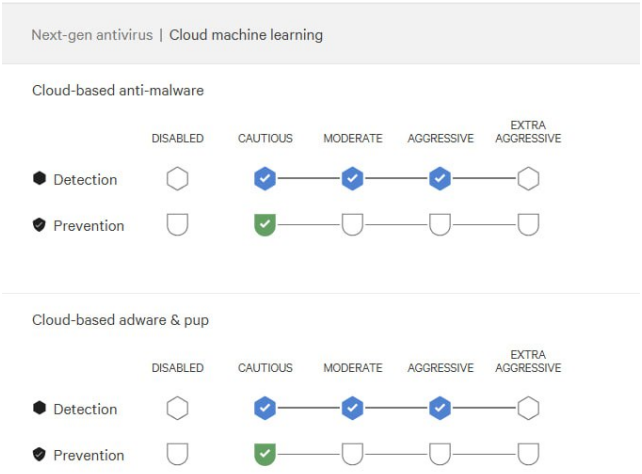

Рисунок 4.14 – Слабкі налаштування протидії в політиці захисту (ч.3)

Однак даний недолік був вчасно виявлений за допомогою симуляції кібератак, а необхідні параметри захисту були увімкнені для налаштування оптимального захисту кінцевого пристрою (рис. 4.15).

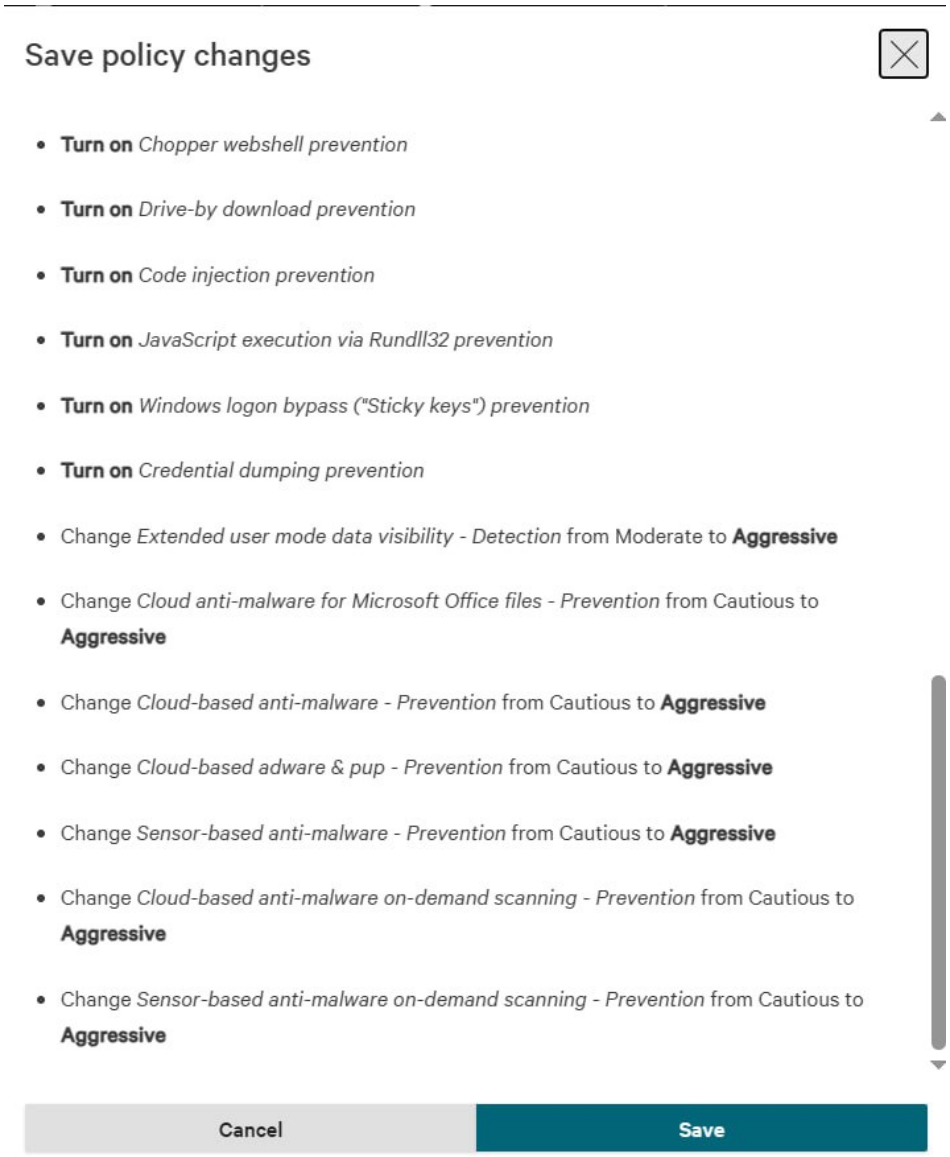

Рисунок 4.15 – Внесені зміни в політику захисту кінцевого пристрою

Після внесення змін, важливо здійснити повторне тестування, щоб переконатись у впливі виконаних змін на результати. Тобто, що система захисту працює як необхідно на даний момент. Після повторного запуску тесту, в консолі можна відразу побачити помилки (рис. 4.16), що свідчать про неуспішність виконуваних тестів, а отже – про успішність нових заходів захисту.

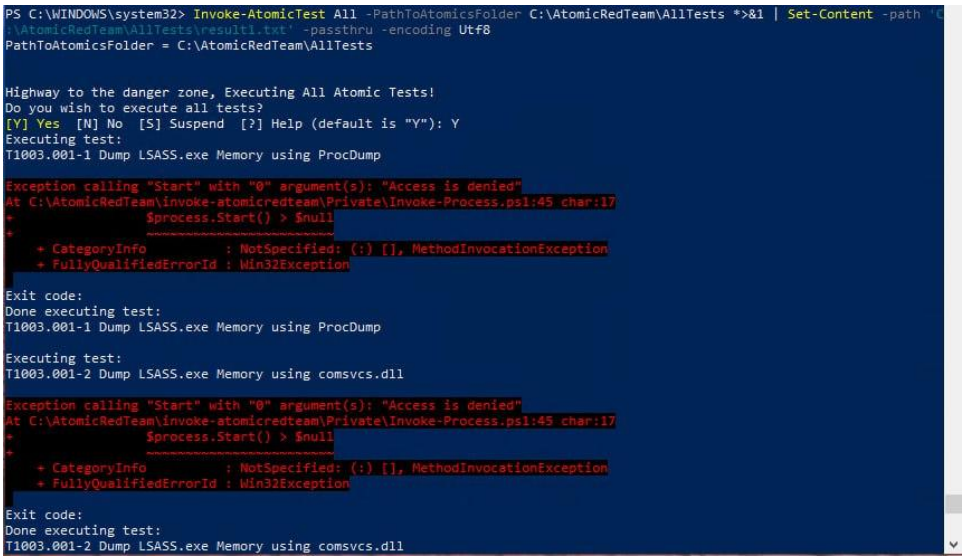

Рисунок 4.16 – Повторний запуск симуляції та помилки при виконанні шкідливих дій

Після завершення симуляції усіх шкідливих дій, в консолі СЗ виконується аналіз результатів. Цього разу виявлень підозрілої активності менше – 118 результатів (рис. 4.17), що свідчить про блокування підозрілої активності на початкових етапах, не даючи їй подальшого розвитку, як це було в попередньому тесті коли блокування не відбувались.

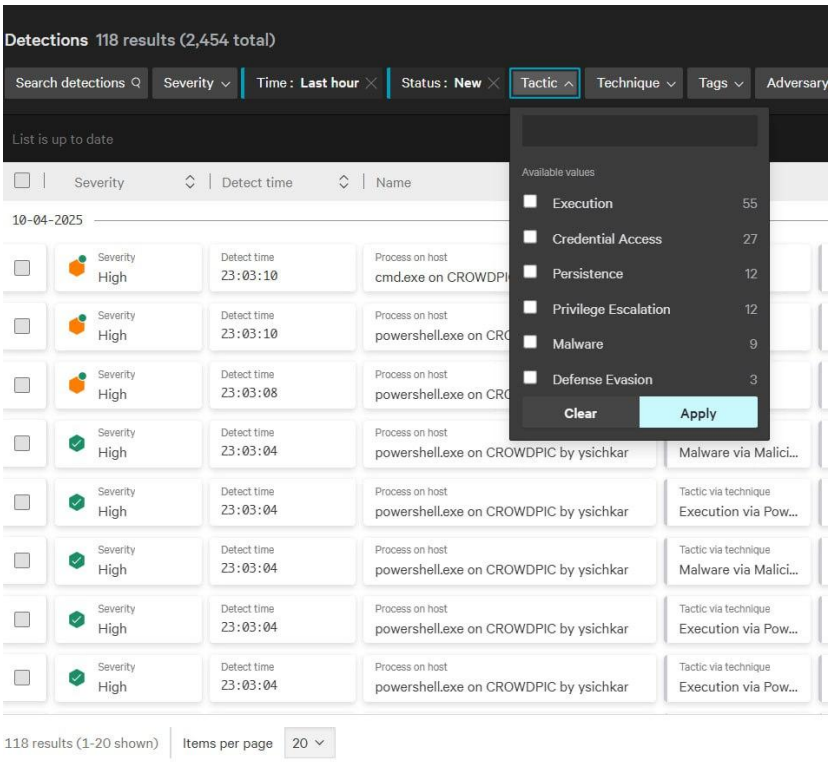

Рисунок 4.17 – Результати повторної симуляції кібератак

Також варто порівняти активність за техніками T1003 та T1548.002, які детальніше розглядали під час попередньої симуляції. Цього разу дана зловмисна активність була заблокована в обох випадках (рис. 4.18, рис. 4.19), про що свідчить повідомлення в системі захисту.

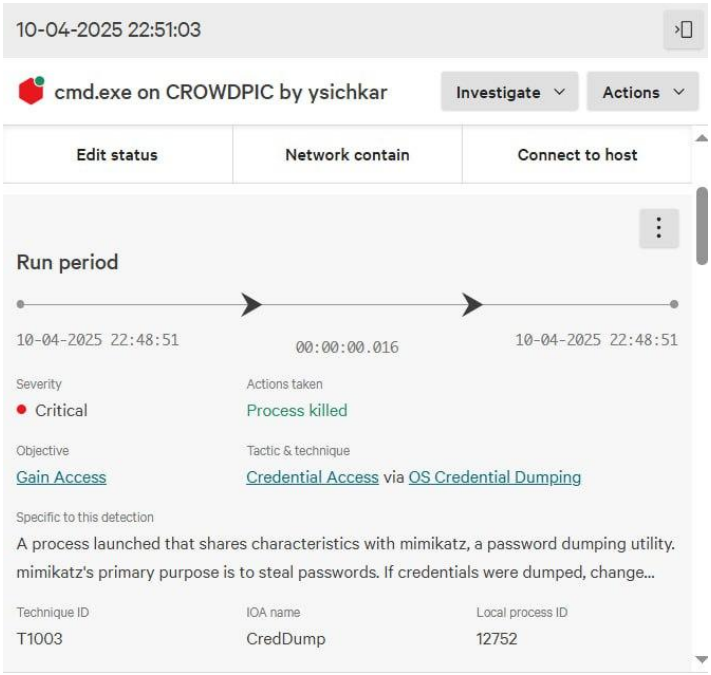

Рисунок 4.18 – Успішне блокування шкідливого процесу, що використовував техніку T1003

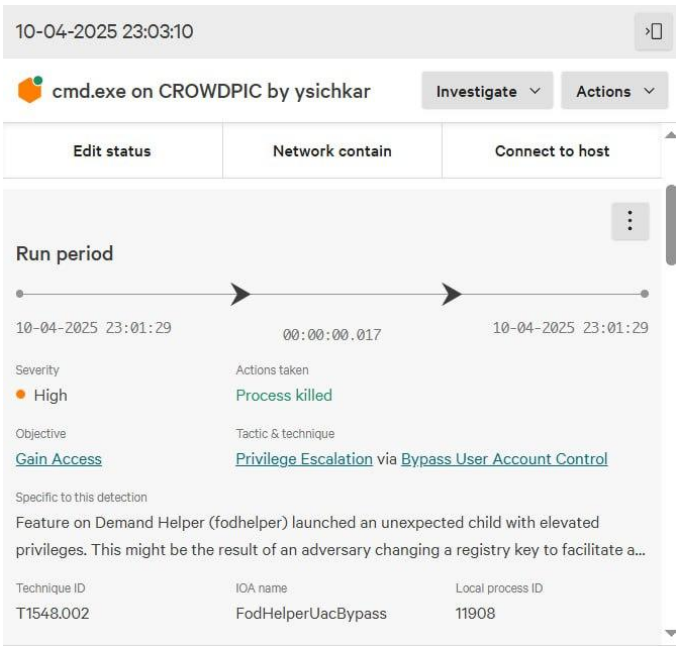

Рисунок 4.19 – Успішне блокування шкідливого процесу, що використовував техніку T1548.002

За результатами симуляції кібератаки вдалось виявити проблеми в політиці захисту EDR системи та вчасно внести необхідні зміни. Однак основним недоліком даного модулю є важкість розробки нових симуляцій, відсутність повного покриття матриці MITRE, обмежені можливості віддаленого запуску симуляцій та відсутність підтвердження блокування шкідливої активності системою симуляції кібератак.

4.2 Використання інструменту MITRE Caldera для регулярної перевірки коректності налаштування EDR системи

Для початку визначимо ціль симуляції — перевірка ефективності захисту кінцевої точки від атак з використанням програм-вимагачів (ransomware). Цей тип шкідливого ПЗ становить одну з найсерйозніших загроз для організацій будь-якого масштабу. Згідно з останніми звітами, атаки з використанням ransomware з кожним роком завдають все більших фінансових збитків, блокуючи доступ до критичних даних та вимагаючи викуп за їх відновлення, що вже було розглянуто в підрозділі 1.1.

Те, як відбуваються подібні атаки, можна також проаналізувати за допомогою відомих тактик, технік і процедур (TTPs), описаних у фреймворку MITRE ATT&CK. Саме тому симуляція подібної атаки дозволяє завчасно виявити недоліки в системах захисту та оперативно їх усунути.

Згаданий у розділі модуль AtomicRedTeam має свої недоліки, тому важливо розглянути більш складне для освоєння рішення – MITRE Caldera, яке в той же час надає ширші можливості та все ще залишається безкоштовним.

MITRE Caldera дозволяє моделювати дії зловмисника в реальному середовищі з використанням агентів та сценаріїв (операцій), які імітують поведінку шкідливого ПЗ, зокрема ransomware. Для цього було розгорнуто сервер Caldera локально (рис. 4.20) та налаштовано відповідного агента на кінцевій точці (рис. 4.21) [82].

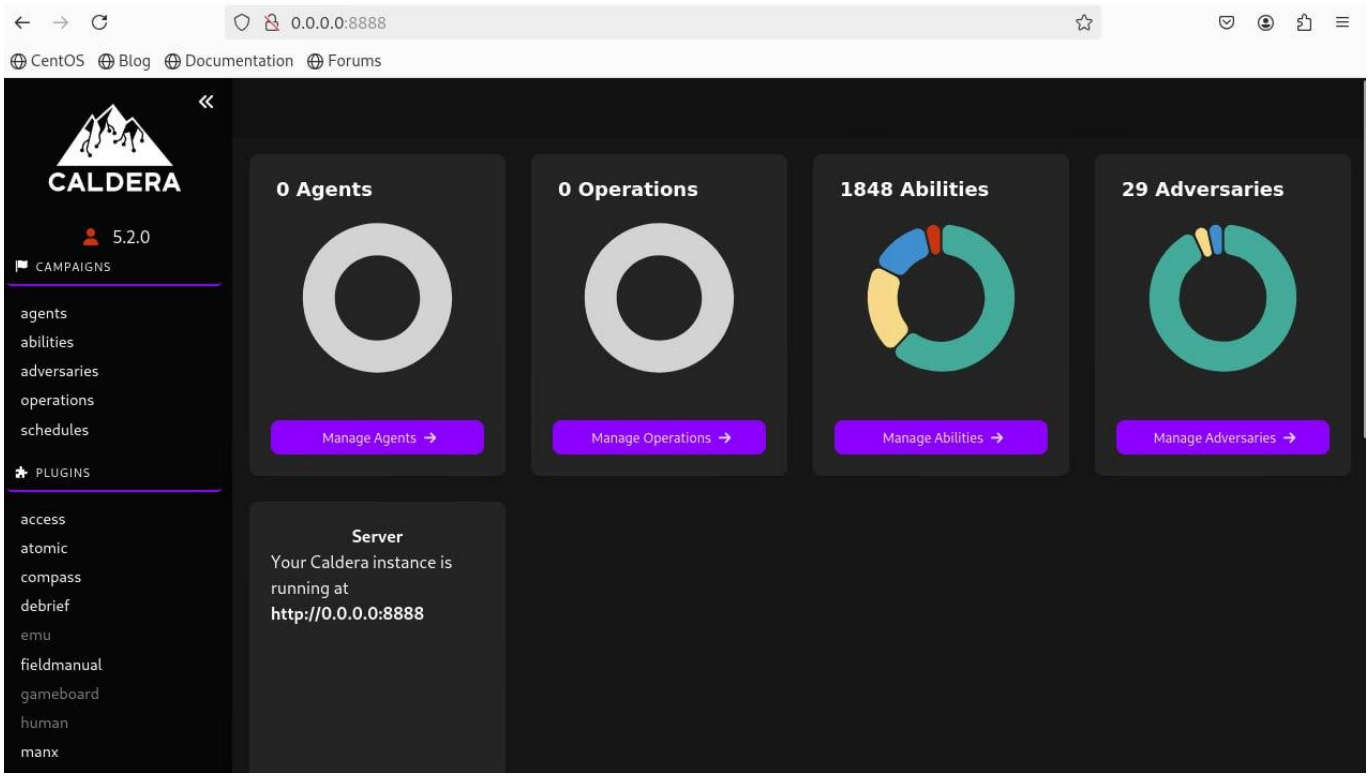

Рисунок 4.20 – Веб-консоль керування системою MITRE Caldera

Рисунок 4.21 – Встановлений агент на хості, готовий до виконання симуляцій

Для формування сценаріїв атак потрібно скласти профіль зловмисника, тому вибираємо дії які будуть релевантними для даного профілю. Система надає можливість вибору широкого спектру дій відразу з їх описом (рис. 4.22), щоб фахівець відразу міг визначити чи підходить дана дія для тестування того чи іншого сценарію.

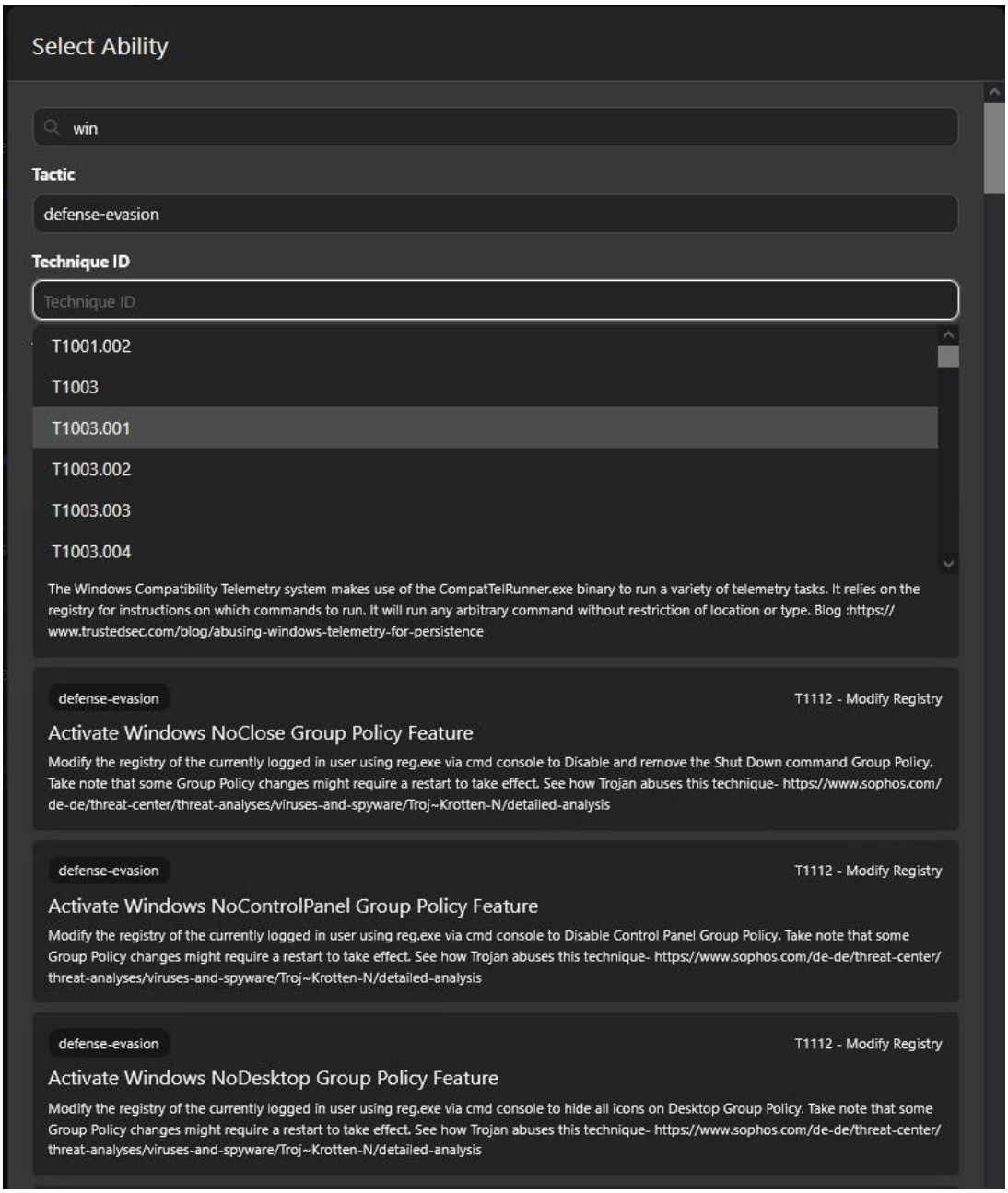

Рисунок 4.22 – Підбір дій, які будуть виконуватись під час симуляції

Додатково система надає можливість створювати власні дії, які можна додати до сценаріїв тестування (рис. 4.23).

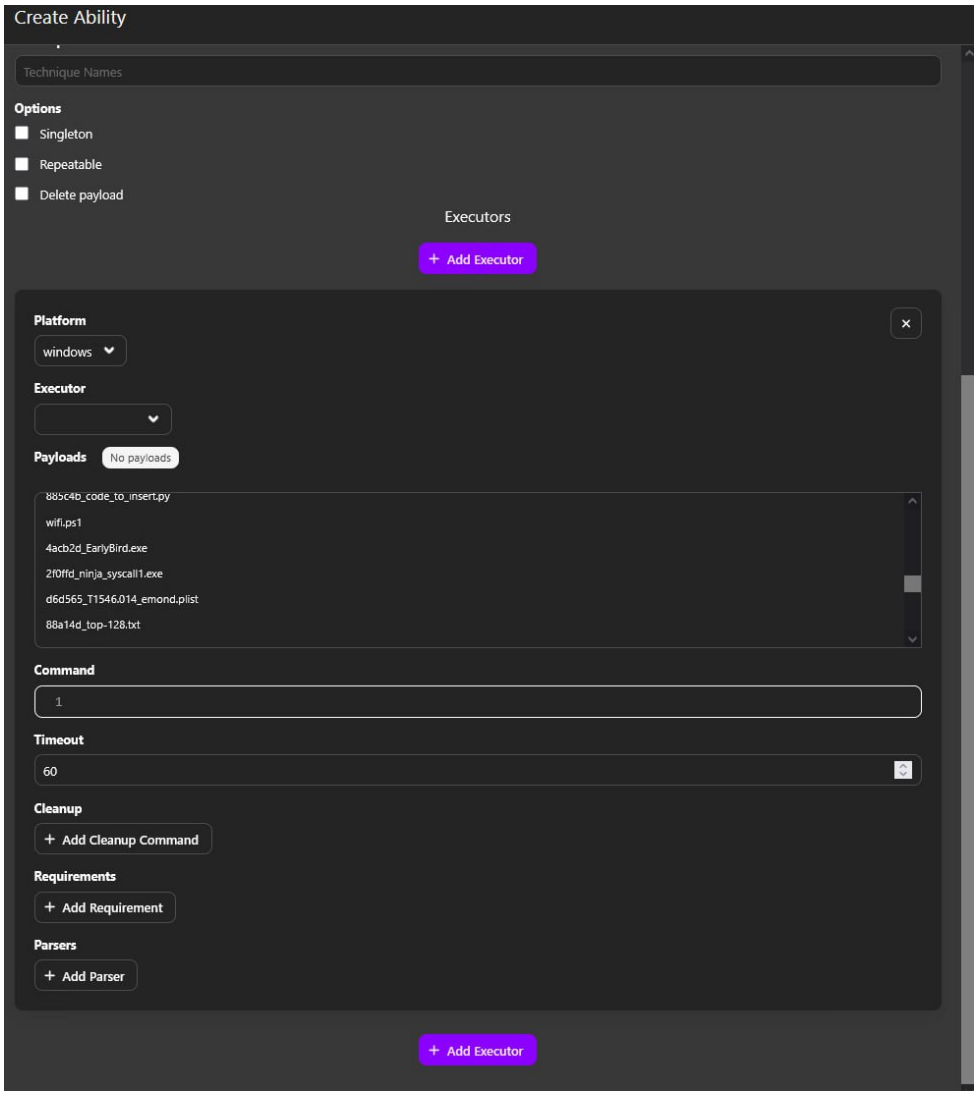

Рисунок 4.23 – Можливість створення власних сценаріїв атак для здійснення симуляцій

В результаті було створено профіль зловмисника «Ransomware» (рис. 4.24) та додано до цього профілю наступні дії:

- Akira Ransomware – Drop Files with .akira Extension and Ransomnote
- BlackByte Ransomware – Registry Changes (CMD)
- BlackByte Ransomware – Registry Changes (PowerShell)
- Ryuk Ransomware Style – Grant Full Access to Folder for Everyone
- PureLocker – Ransom Note
- Scarab Ransomware – Defense Evasion Activities

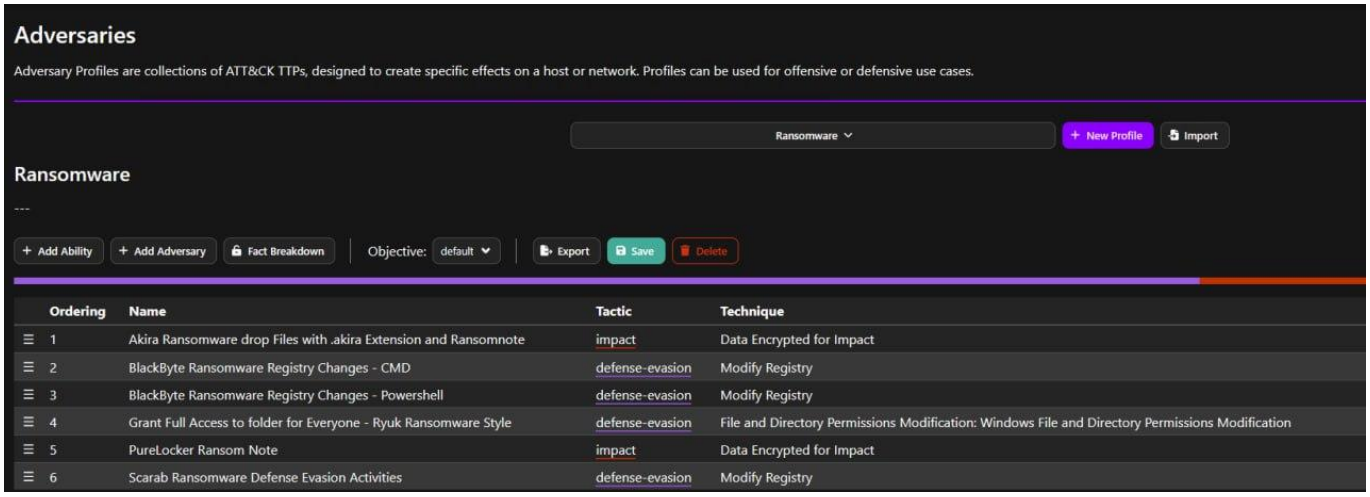

Рисунок 4.24 – Створений профіль зловмисника для симуляції атаки

Однією з важливих можливостей систем симуляції кібератак є виконання регулярних симуляцій, щоб оперативно виявляти будь які відхилення від стандартного значення, яке відображає успішність блокувань. За допомогою MITRE Caldera можна налаштувати, наприклад, щогодинне повторення симуляцій (рис. 4.25).

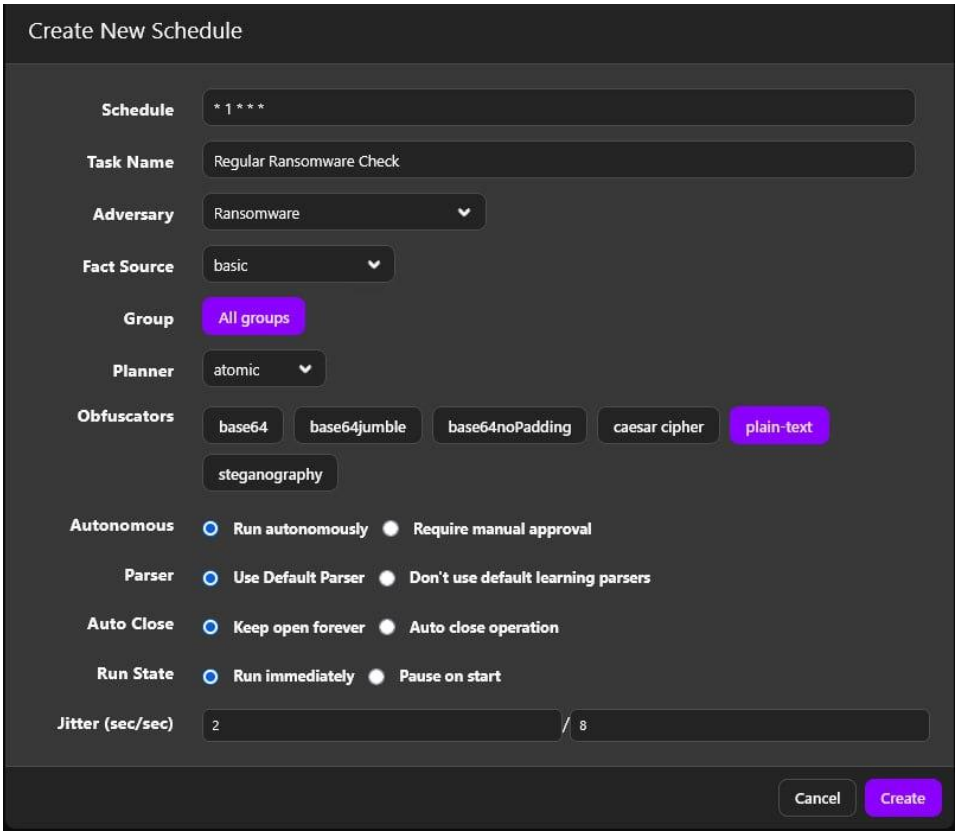

Рисунок 4.25 – Налаштування щогодинного повторення симуляції за створеним профілем зловмисника

Після встановлення агента симуляцій та налаштування необхідного профіля зловмисника, було здійснено запуск симуляції кібератаки для тестування реакції СЗ кінцевих точок CrowdStrike Falcon. За результатами симуляції – усі зловмисні дії були успішно виконані на кінцевому пристрої, в даному випадку система симуляції повідомляє про статус виконуваних дій (рис. 4.26). Відразу можна зробити висновок про некоректність налаштування СЗ.

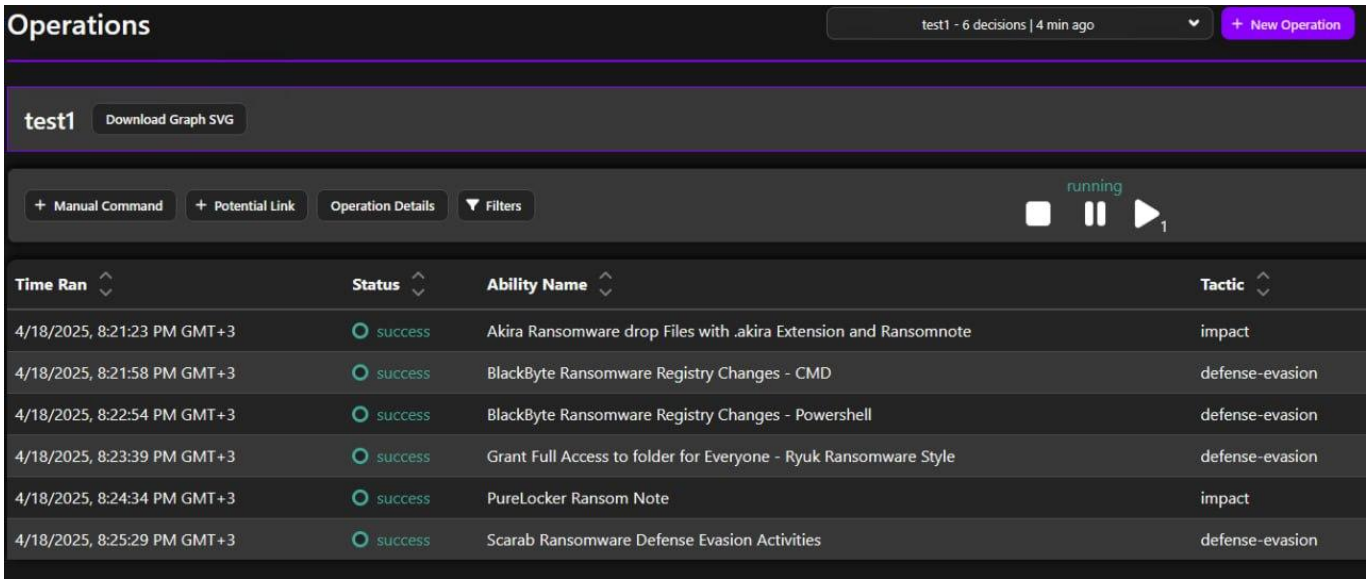

Рисунок 4.26 – Успішне виконання шкідливих команд

Після аналізу спрацювань в системі захисту, можна зробити висновок, що шкідливі дії частково виявляються, однак блокувань не відбувається, що може свідчити про проблеми в налаштуванні політики захисту (рис. 4.27).

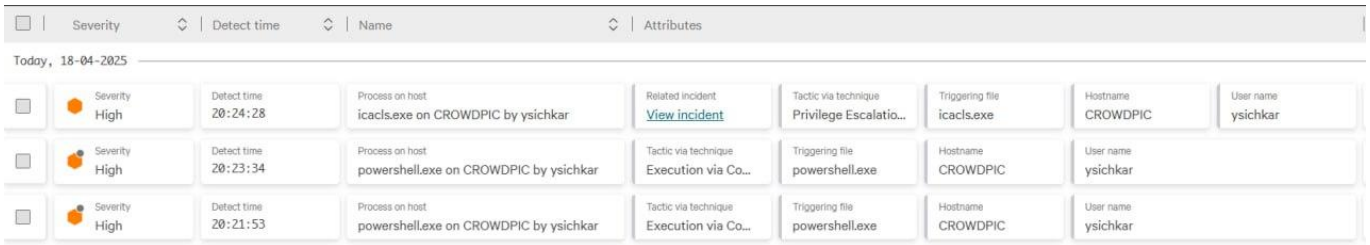

Рисунок 4.27 – Відсутність блокувань підозрілої діяльності в системах захисту

Для блокування шкідливої активності, що пов’язана з шифрувальниками, в багатьох системах захисту присутні окремі параметри для увімкнення. Дані

параметри було вимкнено у політиці, котра була застосована до кінцевого пристрою (рис. 4.28). Варто зауважити, що симуляції мають виконуватись на окремому хості, який має аналогічний захист до інших хостів в групі, наприклад до продуктивних серверів.

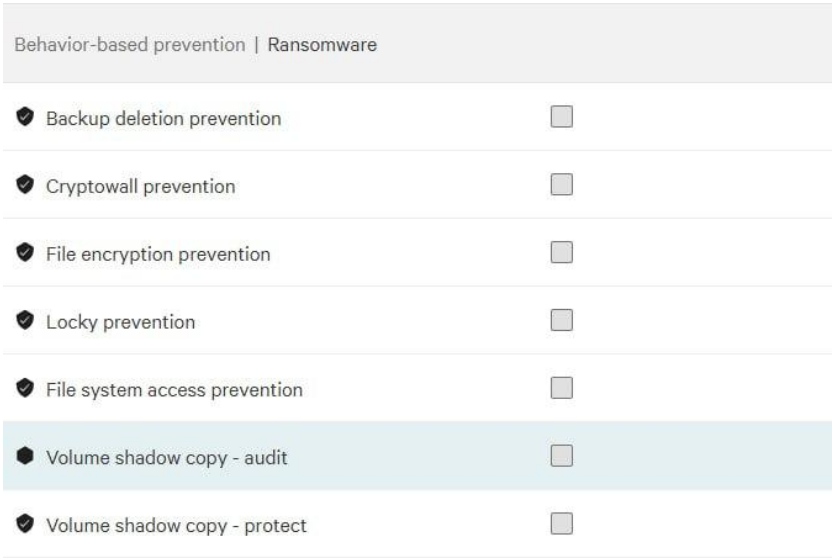

Рисунок 4.28 – Вимкнені параметри захисту від шифрувальників

Після увімкнення необхідних параметрів захисту та розповсюдження політики на всі кінцеві пристрої в групі, було проведено повторне тестування, усі шкідливі дії якого були заблоковані (рис. 4.29). Завдяки використанню MITRE Caldera вдалося оцінити здатність захисних механізмів виявляти й блокувати ключові дії ransomware-атак, було виявлено та усунуто недоліки в системах захисту, що є критично важливим для забезпечення стійкості до інцидентів такого типу.

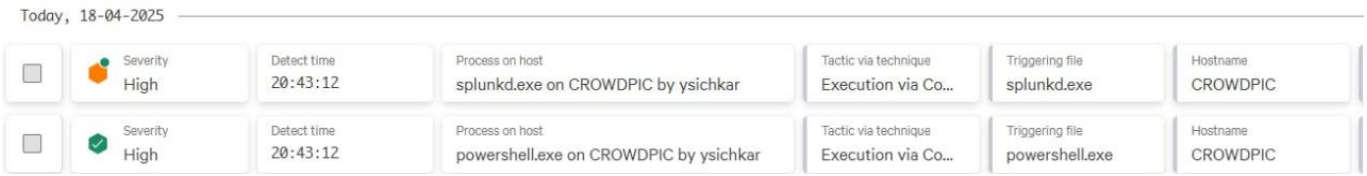

Рисунок 4.29 – Успішне блокування діяльності агента, який виконував симуляцію кібератаки

Основними ж недоліками використання даної системи є складність створення виключень в системах захисту для безперешкодної роботи агента симуляцій, рідкісне додавання нових тестів зі сторони спільноти, що змушує використовувати лише

обмежену кількість тестів або створювати їх власноруч та відсутність рекомендацій для покращення систем захисту.

4.3 Використання платформи Picus для регулярної перевірки систем захисту організації

Для повноцінного ТС захисту за допомогою систем симуляції кібератак можна використати платформу Picus. Дана платформа дозволяє повноцінно протестувати усі наявні СЗ та надати максимальну зручну аналітику з рекомендаціями для покращення даних систем. Окрім великої бібліотеки доступних для симуляції окремих загроз, вендор також пропонує готові набори тестів, які динамічно оновлюються та покращуються, щоб слідувати актуальним загрозам. Наприклад є готові набори тестів, які дозволяють перевірити захист пошти від актуальних загроз, використання яких було розповсюджено під час російсько-української кібервійни та тести рекомендовані CERT-UA (рис. 4.30).

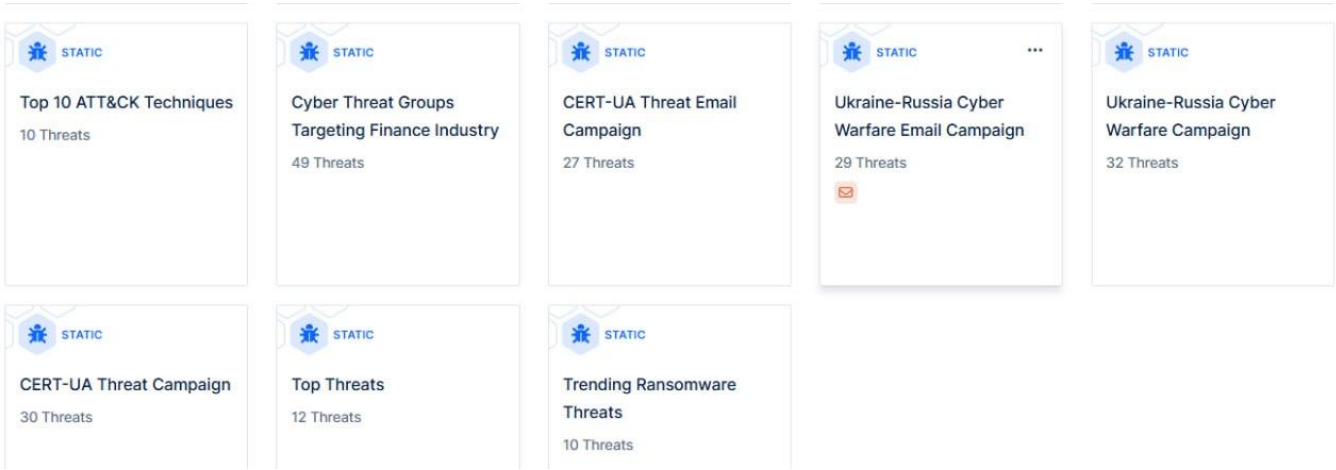

Рисунок 4.30 – Готові набори загроз для здійснення симуляцій

Відповідно в системі є можливість зручного відображення рівня захисту та виявлення на часовому проміжку, що дозволяє легко та зручно виявити будь які відхилення від стандартного значення (рис. 4.31).

Рисунок 4.31 – Зміни рівня захисту та виявлення протягом останнього року

Важливо зазначити, що виявлення та блокування не повинні мати максимального значення у 100%, оскільки не всі дії що відносяться до атак є такими, що потенційно можуть нанести шкоду системі, наприклад це можуть бути дії перегляду імені хоста та звичайні спроби підключення до інших хостів. Дані дії можуть виконуватись під час атаки, але їх блокування та виявлення може свідчити про занадто агресивні політики захисту, котрі можуть спричиняти незручності в стандартній роботі користувачів. Тому рівень захисту і виявлення може варіюватись залежно від цілей організації.

Для симуляції кібератаки візьмемо готовий набір актуальних загроз відповідно до нещодавнього звіту (рис. 4.32) [83].

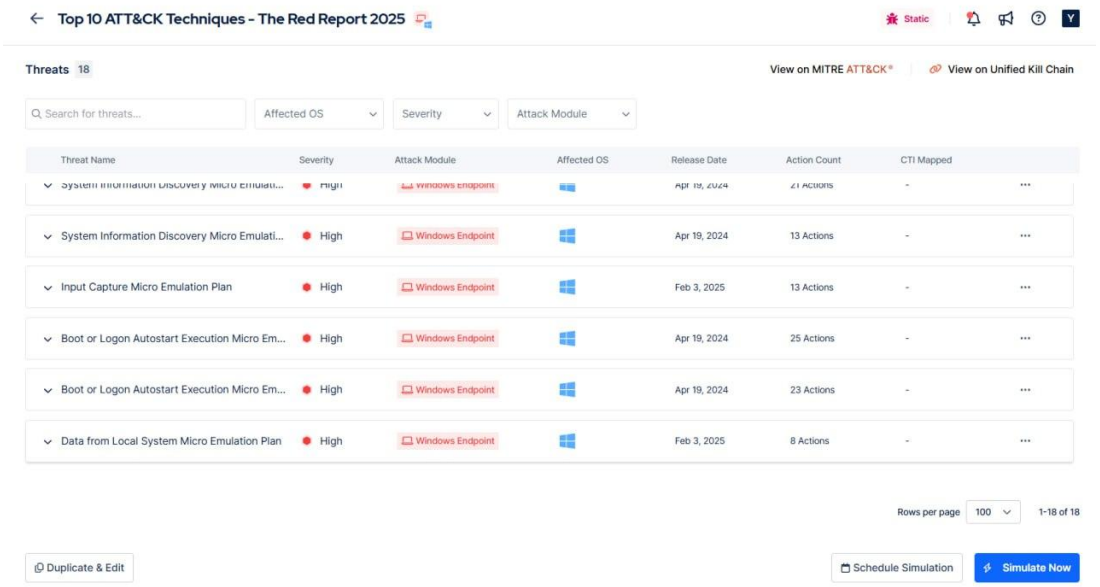

Рисунок 4.32 – Набір тестів відповідно до актуальних загроз

Платформа Picus є хмарним рішенням та потребує лише розгортання агентів симуляцій на кінцевих пристроях, тому її використання є дуже зручним. Також платформа надає можливість інтеграції з системами захисту, що дозволить отримати максимально об’єктивні дані та швидко проаналізувати усі результати атак. Під час налаштування симуляції атаки потрібно обрати попередньо інтегровані системи, в нашому випадку це CrowdStrike Falcon та IBM QRadar SIEM (рис. 4.33).

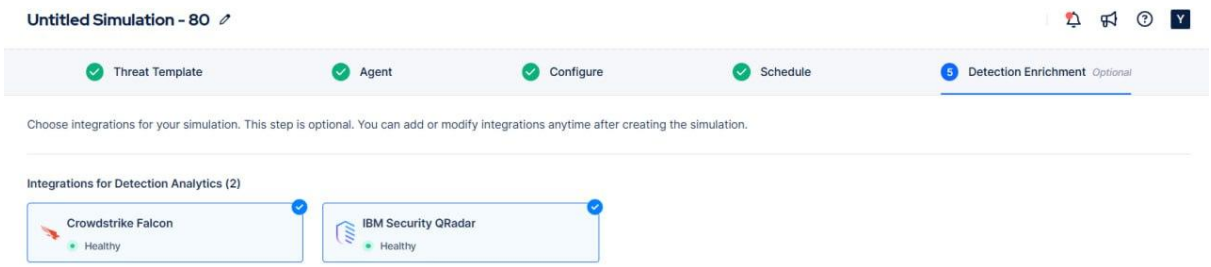

Рисунок 4.33 – Вибір інтеграції для збагачення результатів симуляції

Після проведення симуляції можна виконати аналіз кожної з шкідливих дій. Наприклад визначити що дія не була заблокована, а також за допомогою інтеграцій відразу можна з’ясувати, що в системах захисту дана активність не була залогована, відповідно сповіщень про атаку теж отримано не було (рис. 4.34).

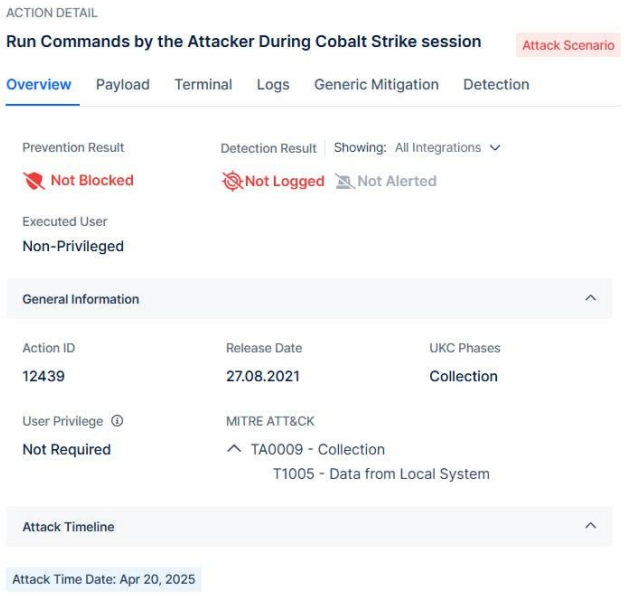

Рисунок 4.34 – Відсутність блокування та логування симульованої зловмисної діяльності

Для покращення результатів захищеності, платформа Picus надає рекомендації щодо покращення захисту від загроз що симулювались. Наприклад можна отримати загальні рекомендації по покращенню рівня кібербезпеки організації, по налаштуванню систем захисту (рис. 4.35) та систем виявлення (рис. 4.36), якщо в організації присутня відповідна підписка на функціонал.

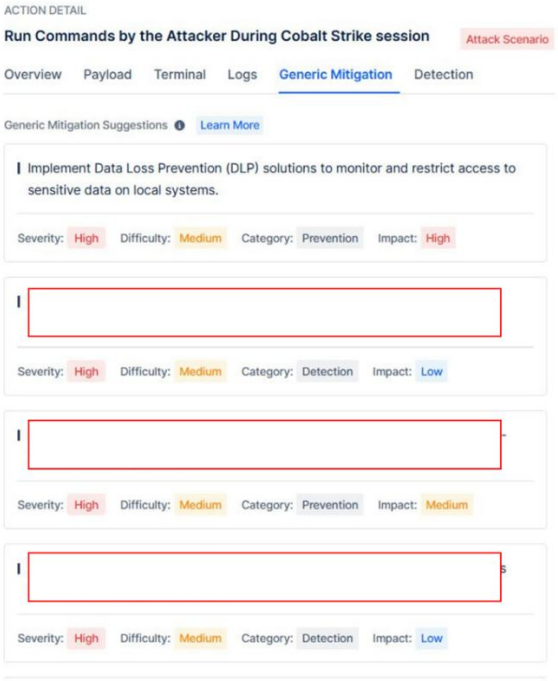

Рисунок 4.35 – Рекомендації по протидії загрозі, яка не була заблокована

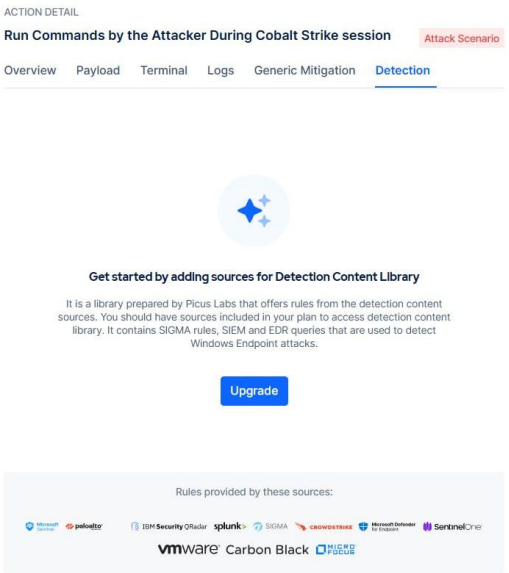

Рисунок 4.36 – Можливість отримати рекомендації по правилах, для виявлення загроз

Додатковою опцією платформи є також можливість перевірити вже наявні правила, які були створені в SIEM системі (рис. 4.37), та виявити потенційні недоліки, як от неправильно налаштовані джерела подій чи некоректно написані правила, що дозволяє комплексно підійти до проблеми недостатнього логування подій.

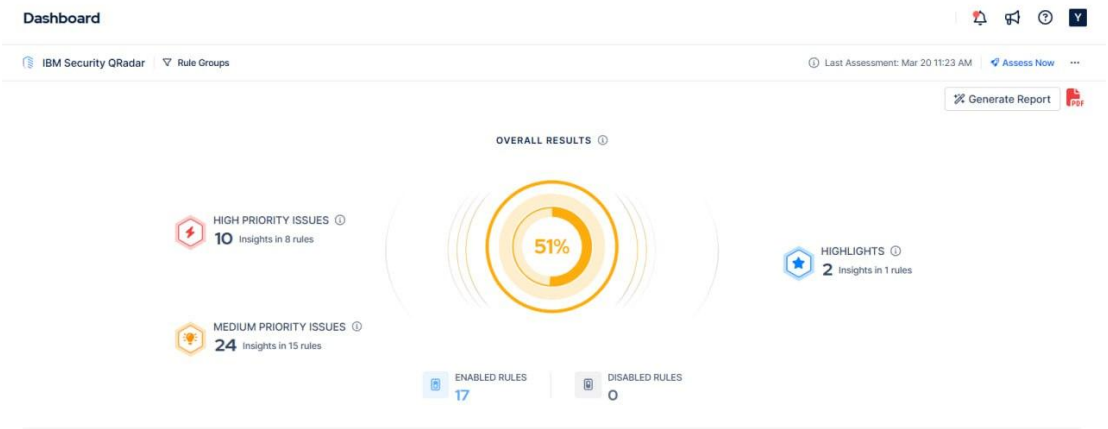

Рисунок 4.37 – Аналітика по правилах, які створені в SIEM системі на даний момент

За результатами симуляції було заблоковано 52% від усіх цілей зловмисників за допомогою CrowdStrike Falcon, в той час як IBM QRadar SIEM виявив 11% від усіх загроз (рис. 4.38).

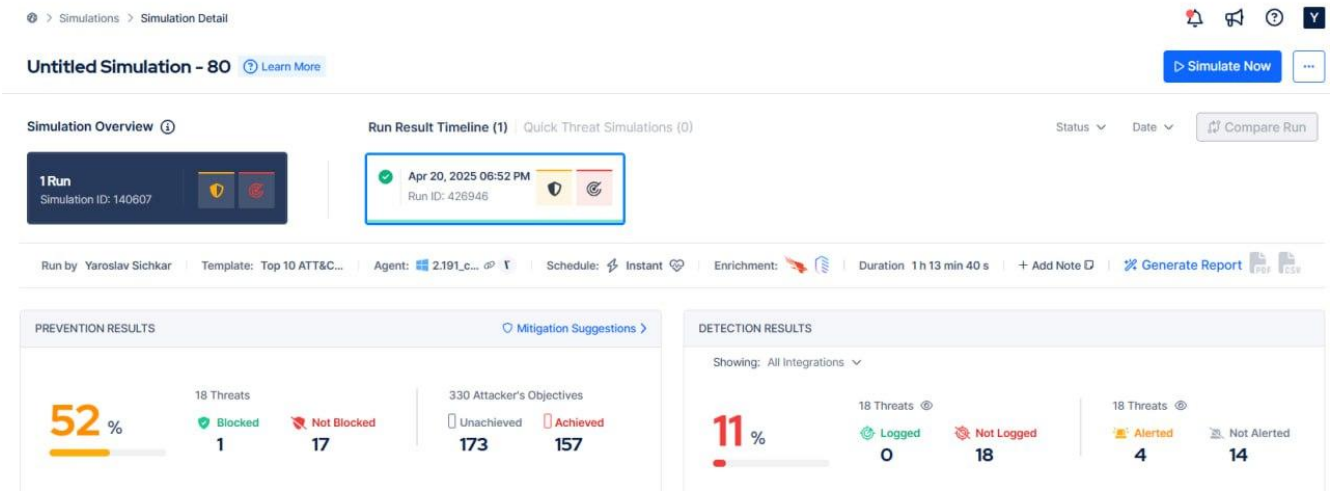

Рисунок 4.38 – Результати симуляції кібератаки

Аналізуючи налаштування СЗ, було виявлено, що до групи кінцевих пристроїв було застосовано занадто широкі виключення, таким чином моніторинг деяких папок

не відбувався. Це могло негативно вплинути на рівень блокування та виявлення, тому дане виключення було видалено і замінено на більш специфічне (рис. 4.39).

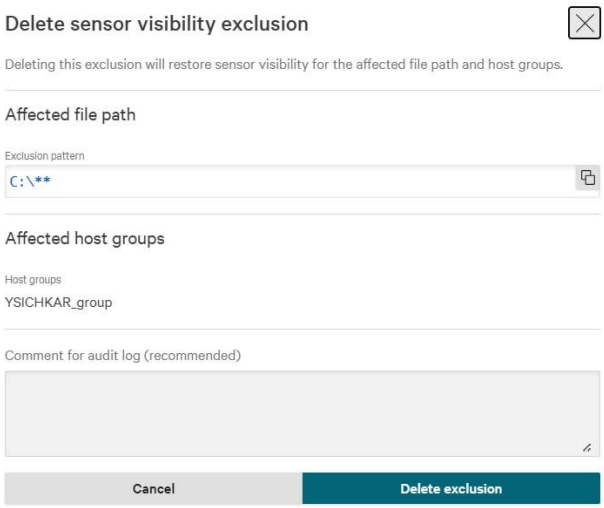

Рисунок 4.39 – Видалення виключення, яке мало вплив на захист пристрою

Здійснивши зміни, було проведено повторну симуляцію, яка підтвердила припущення – відсоток блокувань шкідливих дій зріс до 56% (рис. 4.40).

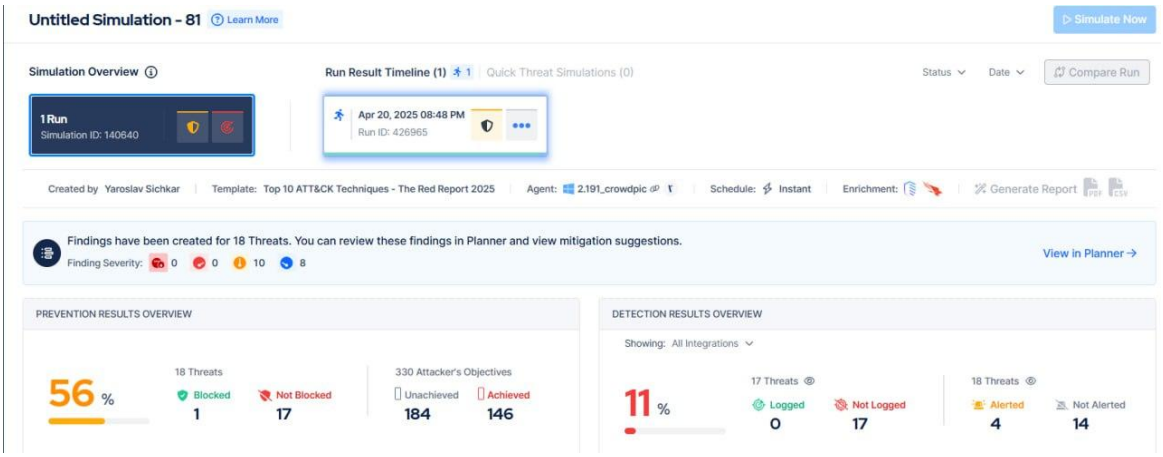

Рисунок 4.40 – Повторна симуляція кібератаки

Також варто звернути увагу, що рівень виявлення загроз не змінився і досі залишається низьким. Це вимагає негайного реагування, збагачення SIEM системи подіями з кінцевих пристроїв та створення правил виявлення. З цим також може допомогти платформа Picus. Як вже було розглянуто, регулярна симуляція, виконання

рекомендацій платформи та повторне тестування, можуть докорінно змінити готовність організації до реальних кібератак.

Цінність методу тестування систем захисту за допомогою симуляції кібератак на практиці підтверджує звіт АТ «Укртелеком» [84], згідно якого, за допомогою платформи Picus організація змогла значно розширити можливість своєї SIEM системи.

Висновки до четвертого розділу

Симуляція кібератак є невід'ємною складовою сучасного підходу до забезпечення кібербезпеки, оскільки дає змогу оцінити ефективність систем захисту в реальних умовах. Застосування інструментів, таких як AtomicRedTeam, MITRE Caldera та Picus, дозволяє відтворювати різноманітні сценарії атак на основі матриці MITRE ATT&CK, що охоплює всі фази атаки — від первинного доступу до ексфільтрації даних. Це забезпечує глибоке розуміння поведінки зловмисників та дозволяє виявляти слабкі місця в існуючих засобах захисту.

Кожна з систем має власні переваги та недоліки та дозволяє не лише оцінювати здатність до виявлення атак, а й перевіряти ефективність процесів реагування. Проведення таких симуляцій допомагає виявити прогалини в кібербезпеці організації, недоліки в налаштуваннях систем, а також потенційні організаційні проблеми, що можуть вплинути на здатність до реагування на інциденти.

У результаті тестування методу було доведено, що СЗ можуть ефективно протидіяти загрозам, але їхня ефективність значною мірою залежить від коректності конфігурації, якості правил виявлення та достатнього збагачення подіями. Аналіз результатів тестувань надав можливість сформулювати рекомендації щодо підвищення рівня захисту інформаційної інфраструктури.

Таким чином, симуляція атак із використанням спеціалізованих систем симуляції кібератак є потужним інструментом не лише для ТС безпеки, а й для вдосконалення політик безпеки та підвищення обізнаності персоналу. Її регулярне проведення сприяє створенню стійкої до загроз системи кіберзахисту.

ВИСНОВОК

Враховуючи стрімкий розвиток кіберзагроз та методів атак з боку зловмисників, які використовують сучасні технології включно зі штучним інтелектом, питання постійного тестування систем захисту набуває особливої актуальності. Традиційні методи перевірки, такі як пентест і Red Teaming, мають низку обмежень, зокрема епізодичність перевірок, значну залежність від людського чинника та складність охоплення широкого спектра загроз. Тому в роботі було досліджено сучасні підходи до безперервного тестування кіберзахисту за допомогою автоматизованої симуляції атак.

У першому розділі було проаналізовано актуальність використання симуляцій кібератак у контексті зростаючих загроз, зокрема проти критичної інфраструктури. Розглянуто недоліки традиційних методів тестування, що обумовлює потребу у впровадженні нових підходів, орієнтованих на проактивне виявлення недоліків в системах захисту і перевірку готовності до інцидентів.

У другому розділі виконано порівняння сучасних підходів до перевірки ефективності засобів кіберзахисту, зокрема BAS, Red Teaming, пентестинг та аудити безпеки. Кожен з методів має свої особливості, частоту застосування, вартість, що визначає його доцільність у певному контексті. Симуляція кібератак дозволяє проводити регулярну перевірку захисту, тоді як Red Team дає змогу оцінити стійкість до складних і нетипових атак. Комплексне використання зазначених підходів підвищує ефективність управління кіберризиками та сприяє забезпеченню проактивного захисту.

У третьому розділі розроблено метод тестування систем захисту з використанням автоматизованої симуляції кібератак та розглянуто ключові аспекти реалізації методу від вибору інструментів до побудови сценаріїв на основі реальних технік атак. Наголошено на важливості інтеграції систем симуляцій кібератак з інструментами захисту (SIEM, EDR, SOAR та іншими) та використання результатів для вдосконалення політик і процедур безпеки.

У четвертому розділі проведено практичну перевірку методу тестування систем захисту за допомогою симуляції кібератак із використанням інструментів AtomicRedTeam, MITRE Caldera та Picus. Це дозволило оцінити ефективність EDR-систем та SIEM у реальних умовах на основі тактик та технік MITRE ATT&CK. Аналіз результатів засвідчив, що ефективність захисту значною мірою залежить від коректної конфігурації систем, актуальності правил виявлення та здатності до швидкого реагування. На основі проведених симуляцій сформовано рекомендації для підвищення рівня захищеності.

Таким чином, у дипломній роботі було обґрунтовано доцільність впровадження безперервного тестування систем захисту за допомогою симуляцій кібератак, як одного з сучасних підходів до оцінки та вдосконалення систем кібербезпеки. Отримані результати можуть бути використані для подальших досліджень, розробки політик безпеки та покращення існуючих засобів захисту.

У ході виконання поставленої мети, яка полягала у розробці методу тестування систем захисту з використанням симуляції кібератак, всі завдання виконані у повному обсязі:

1) Здійснено порівняльний аналіз систем симуляції кібератак з традиційними методами тестування систем захисту та зроблено висновок про доцільність використання комбінованого підходу.

2) Розглянуто системи симуляції кібератак, як вони допомагають виявити недоліки в системах захисту та переваги інтеграції таких систем із існуючими системами кібербезпеки.

3) Розроблено метод тестування систем захисту з використанням автоматизованої симуляції кібератак, описано етапи даного методу: від планування до повторного тестування.

4) Проведено тестування систем захисту за допомогою симуляції кібератак, в результаті чого було виявлено їх недоліки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cyber security for SMBs: Navigating Complexity and Building Resilience. Sage. URL: https://www.sage.com/en-gb/company/digital-newsroom/2023/10/12/cyber-security-for-navigating-complexity-and-building-resilience/ (дата звернення: 16.03.2025)

2. Infographic: cybercrime expected to skyrocket in coming years. *Statista Daily Data*. URL: https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/ (дата звернення: 16.03.2025).

3. 2024 ransomware report: sophos state of ransomware. *SOPHOS*. URL: https://www.sophos.com/en-us/content/state-of-ransomware (дата звернення: 16.03.2025).

4. CERT-UA минулого року опрацювала 4315 кіберінцидентів. *Державна служба спеціального зв'язку та захисту інформації України*. URL: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv.

5. Тарасовський Ю. Хакери перебували в системі «Київстару» з травня 2023 року. СБУ розкрила деталі кібератаки – *Forbes.ua. Forbes.ua | Бізнес, мільярдери, новини, фінанси, інвестиції, компанії.* URL: https://forbes.ua/news/khakeri-perebuvali-v-sistemi-kiivstar-z-travnya-2023-roku-sbu-04012024-18307 (дата звернення: 16.03.2025).

6. Key cyber security statistics for 2025. *SentinelOne*. URL: https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-statistics/ (дата звернення: 16.03.2025).

7. ChatGPT is creating new risks for national security. *Defense News*. URL: https://www.defensenews.com/opinion/2023/07/20/chatgpt-is-creating-new-risks-for-national-security/ (дата звернення: 16.03.2025).

8. Каун Ю., Собчук О. Штучний інтелект як інструмент кібератак і кібербезпеки. І Міжнародна науково-практична конференція «Проблеми

комп'ютерних наук, програмного моделювання та безпеки цифрових систем». 2024. С. 40–41.

9. Howarth J. 8 Top Cybersecurity Industry Trends (2024). *Exploding Topics*. [Електронний ресурс]. URL: https://explodingtopics.com/blog/cybersecurity-trends (дата звернення: 16.03.2025).

10. Kibet A., Esquivel R. Ransomware: Ransomware As A Service (Raas), Methods To Detects, Prevent, Mitigate And Future Direction. *ResearchGate*. URL: https://www.researchgate.net/publication/365349176_RANSOMWARE_RANSOMWARE_AS_A_SERVICE_RaaS_METHODS_TO_DETECTS_PREVENT_MITIGATE_AND_FUTURE_DIRECTION.

11. Mandadi S., Prasad Gochhayat S. Cybersecurity risks in remote work and learning environments and methods of combating them. Journal of student research. 2024. Т. 13, № 2. С. 1–11.

12. Nobles C. Investigating cloud computing misconfiguration errors using the human factors analysis and classification system. Scientific bulletin. 2022. Т. 27, № 1. С. 59–66.

13. Staff E. India Sees 409% Jump In Cryptojacking Attacks While Five Cyber Security Tactics Ruling the Global Business: Report | Entrepreneur. *Entrepreneur*. URL: https://www.entrepreneur.com/en-in/technology/india-sees-409-jump-in-cryptojacking-attacks-while-five/478028 (дата звернення: 16.03.2025).

14. Mutombo E. N., Tokmak M., Wa Nkongolo M. Cryptojacking detection using local interpretable model-agnostic explanations. *Cryptology ePrint Archive*. URL: https://eprint.iacr.org/2025/050.pdf (дата звернення: 16.03.2025).

15. 2025 Cybersecurity Trends: 7 Trends to Watch | Splunk. *Splunk*. URL: https://www.splunk.com/en_us/blog/learn/cybersecurity-trends.html (дата звернення: 16.03.2025).

16. Митропан А. Кіберзагрози для бізнесу: основні ризики та поради для захисту. *Speka - онлайн-медіа про підприємництво та технології | SPEKA.media | SPEKA.media*. URL: https://speka.media/kiberzagrozi-dlya-biznesu-osnovni-riziki-ta-poradi-dlya-zaxistu-vrxz52 (дата звернення: 23.04.2025).

17. Криклій О. А. Теорія та практика забезпечення кіберстійкості банків. *SumDU Repository: Home*. URL: https://essuir.sumdu.edu.ua/bitstream-download/123456789/82838/1/Krykli_cyber%20threats.pdf (дата звернення: 23.04.2025).

18. Що таке витік даних? | Захисний комплекс Microsoft. *microsoft.com*. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-a-data-leak (дата звернення: 23.04.2025).

19. Cost of a data breach 2024 | IBM. *IBM - United States*. URL: https://www.ibm.com/reports/data-breach (дата звернення: 23.04.2025).

20. Cybersecurity: protect your business from digital threats today | hideez. *Passwordless Workforce Identity Solutions | Hideez*. URL: https://hideez.com/en-ua/blogs/news/how-to-protect-your-business-from-digital-threats?srsltid=AfmBOopQMz6qYelIZj2Xb_ctKc-_M7exaPKSvT4b-GNRoXi0ypDVPt9y (дата звернення: 23.04.2025).

21. How cyberattacks hurt business reputation. *Anapaya | Secure, resilient, and controlled connectivity with SCION*. URL: https://www.anapaya.net/blog/5-ways-cyberattacks-can-damage-a-companys-reputation (дата звернення: 23.04.2025).

22. Software secured | data breach fines: what you need to know | USA. *Software Secured - B2B Manual Penetration Testing Provider USA*. URL: https://www.softwaresecured.com/post/what-is-the-fine-for-data-breaches (дата звернення: 23.04.2025).

23. The hidden impact of cyber attacks on mental health. *Acronym Solutions | Ontario's Top IT & Tech Services*. URL: https://acronymsolutions.com/resources/the-hidden-impact-of-cyber-attacks-on-mental-health/ (дата звернення: 23.04.2025).

24. ISO 27001 penetration testing – A comprehensive guide 2023. *Qualysec*. URL: https://qualysec.com/iso-27001-penetration-testing-a-comprehensive-guide-2023/ (дата звернення: 23.04.2025).

25. PCI DSS checklist: 12 most important requirements. *SISA*. URL: https://www.sisainfosec.com/blogs/pci-dss-4-0-checklist-12-most-important-requirements-explained/ (дата звернення: 23.04.2025).

26. PCI DSS – requirement 11 – regularly test security systems and processes. *ISMS.online*. URL: https://www.isms.online/pci-dss/requirement-11/ (дата звернення: 23.04.2025).

27. PCI penetration testing guide – All you need to know. *Blaze*. URL: https://www.blazeinfosec.com/post/pci-penetration-testing-guide/.

28. GDPR penetration testing: navigating compliance safely. *astra*. URL: https://www.getastra.com/blog/compliance/gdpr/gdpr-penetration-testing/ (дата звернення: 23.04.2025).

29. Why do penetration testing for GDPR? Article 32 & much more. *Network Assured*. URL: https://networkassured.com/compliance/penetration-testing-for-gdpr/ (дата звернення: 23.04.2025).

30. Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем : НД ТЗІ 2.3-025-24.

31. Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення. *ТЗІ - інформаційна безпека та захист інформації*. URL: https://tzi.com.ua/downloads/2.1-002-07.pdf (дата звернення: 23.04.2025).

32. Захист інформації. Технічний захист інформації. Основні положення. *ТЗІ - інформаційна безпека та захист інформації*. URL: https://tzi.com.ua/downloads/DSTU%203396.0-96.pdf (дата звернення: 23.04.2025).

33. Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/257-2023-п#Text (дата звернення: 23.04.2025).

34. Що таке тестування на проникнення? Повний огляд процедури | ESKA Блог. *ESKA*. URL: https://eska.global/blog/sho-take-testuvannya-na-proniknennya-povnij-oglyad-proceduri (дата звернення: 23.04.2025).

35. Пентест від А до Я: посібник з тестування на проникнення. *KR. Laboratories*. URL: https://kr-labs.com.ua/blog/testuvannya-na-pronyknennya-pentest-vid-a-do-ya/ (дата звернення: 23.04.2025).

36. Методологія пентесту: 5 кращих методологій | Datami. *Datami.ee*. URL: https://datami.ee/ua/blog/top-5-methodologies/ (дата звернення: 23.04.2025).

37. Що таке пентест?. *ITS Red Team*. URL: https://its-red.team/what-is-a-pentest (дата звернення: 23.04.2025).

38. Ornitz S. When should you use red teaming instead of penetration testing (and vice versa)?. *Cymulate*. URL: https://cymulate.com/blog/red-teaming-vs-penetration-testing/ (дата звернення: 23.04.2025).

39. Red teaming – what is it and do you need it? - twelvesec. *Twelvesec*. URL: https://twelvesec.com/2025/02/05/red-teaming-what-is-it-and-do-you-need-it (дата звернення: 23.04.2025).

40. Singh H. What is red teaming: benefits, process, & cost. *thecyphere*. URL: https://thecyphere.com/blog/red-teaming (дата звернення: 23.04.2025).

41. Mindgard. The complete guide to red teaming: process, benefits & more - mindgard. *Mindgard - Automated AI Red Teaming & Security Testing*. URL: https://mindgard.ai/blog/red-teaming (дата звернення: 23.04.2025).

42. What is red teaming and how does it work?. *Application Security Software (AppSec) | Black Duck*. URL: https://www.blackduck.com/glossary/what-is-red-teaming.html (дата звернення: 23.04.2025).

43. What is red teaming & how it benefits orgs. *Trend Micro*. URL: https://www.trendmicro.com/en_sg/research/23/a/what-is-red-teaming.html (дата звернення: 23.04.2025).

44. Miller M. Advantages and disadvantages of red team engagements. *Triaxiom Security*. URL: https://www.triaxiomsecurity.com/advantages-and-disadvantages-of-red-team-engagements/ (дата звернення: 23.04.2025).

45. Red-Teaming in AI: what it is, why it matters, and the challenges it raises – AI plain and simple. *AI Plain And Simple*.

URL: https://www.aiplainandsimple.com/articles/redteaming-in-ai-what-why-and-challenges-it-raises (дата звернення: 23.04.2025).

46. Внутрішній аудит за стандартом ISO: чому це важливо для вашої компанії. *System Management - Certification services*. URL: https://isocert.org.ua/2024/09/26/vnutrishniy-audyt-za-standartom-iso-chomu-tse-vazhlyvo-dlya-vashoyi-kompaniyi/ (дата звернення: 23.04.2025).

47. 5 головних причин, чому внутрішній аудит важливий. *ФОКУС*. URL: https://fokus.com.ua/czikavo/5-golovnyh-prychyn-chomu-vnutrishnij-audyt-vazhlyvyj/ (дата звернення: 23.04.2025).

48. Типові помилки під час внутрішнього аудиту ISO та як їх уникнути. *System Management - Certification services*. URL: https://isocert.org.ua/2024/09/30/typovi-pomylky-pid-chas-vnutrishn′oho-audytu-iso-ta-yak-yikh-unyknuty/ (дата звернення: 23.04.2025).

49. How often should you perform A penetration test?. *PurpleSec*. URL: https://purplesec.us/learn/how-often-perform-penetration-test/ (дата звернення: 23.04.2025).

50. Singh H. What is red teaming: benefits, process, & cost. *thecyphere*. URL: https://thecyphere.com/blog/red-teaming (дата звернення: 23.04.2025).

51. Baran E. A cheap penetration test can cost you more in the end. *blazeinfosec*. URL: https://www.blazeinfosec.com/post/cheap-penetration-test-dangers/ (дата звернення: 23.04.2025).

52. How to reduce your mean time to remediate A vulnerability. *PurpleSec*. URL: https://purplesec.us/learn/mean-time-remediate-vulneraiblity/ (дата звернення: 23.04.2025).

53. Morrow S. Time to patch: vulnerabilities exploited in under five minutes?. *Infosec*. URL: https://www.infosecinstitute.com/resources/vulnerabilities/time-to-patch-vulnerabilities-exploited-in-under-five-minutes/ (дата звернення: 23.04.2025).

54. Global Risks Report 2022: Digital Dependencies and Cyber Vulnerabilities. *weforum.org*. URL: https://www.weforum.org/publications/global-risks-report-2022/in-full/chapter-3-digital-dependencies-and-cyber-vulnerabilities/.

55. Muncaster P. Organizations Now Have an Average 76 Security Tools to Manage. *Infosecurity Magazine*. URL: https://www.infosecurity-magazine.com/news/organizations-76-security-tools/ (дата звернення: 16.03.2025).

56. The Challenge of Utilizing Multiple Security Tools. *Security and IT Operations Platform Powered by AI I Anomali*. URL: https://www.anomali.com/blog/more-is-less-the-challenge-of-utilizing-multiple-security-tools (дата звернення: 16.03.2025).

57. Тренди та найкращі практики кібербезпеки. *Agiliway - Custom Software Development Company*. URL: https://www.agiliway.com/uk-ua/trendy-ta-naykrashchi-praktyky-kiberbezpeky-vidpovidnist-innovatsiyi-ta-zapobihannya-zahrozam/ (дата звернення: 23.04.2025).

58. Моделювання зломів і атак. *IITD*. URL: https://iitd.ua/modelyuvannya-zlomiv-i-atak-bas/ (дата звернення: 23.04.2025).

59. Лучик С., Мойко О. Моделювання кібератак в кіберпросторі. *KhNUIAIR :: Репозитарій ХНУВС*. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/2f841b24-08ed-40e6-b5b9-4e511a48e8d5/content (дата звернення: 16.03.2025).

60. MITRE ATT&CK®. *MITRE ATT&CK®*.. URL: https://attack.mitre.org/ (дата звернення: 15.03.2025).

61. Крет Т. Підходи до моделювання загроз під час створення комплексної СЗ інформації для багаторівневих інтелектуальних систем керування. *Academic Journals and Conferences* |. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2024/jun/34961/vsezdoi-83-90.pdf (дата звернення: 16.03.2025).

62. What are breach and attack simulation (BAS) tools?. *Gartner*. URL: https://www.gartner.com/reviews/market/breach-and-attack-simulation-bas-tools (дата звернення: 23.04.2025).

63. Hamdan M. Threat emulation explained | understanding hacker’s mentality | tryhackme intro to threat emulation. *Medium*. URL: https://motasemhamdan.medium.com/threat-emulation-explained-understanding-hackers-mentality-tryhackme-intro-to-threat-emulation-e2b3b248f0b7 (дата звернення: 23.04.2025).

64. APT29 | MITRE ATT&CK®. *MITRE ATT&CK®*. URL: https://attack.mitre.org/groups/G0016/ (date of access: 23.04.2025).

65. Attack simulation vs attack emulation: what's the difference?. *rThreat*. URL: https://rthreat.net/2021/04/14/blog-attack-simulation-vs-attack-emulation/ (дата звернення: 23.04.2025).

66. Purple teaming explained | simspace cybersecurity insights. *SimSpace*. URL: https://simspace.com/blog/what-is-the-purple-team-in-cybersecurity-purple-teaming-explained-simspace/ (дата звернення: 23.04.2025).

67. Miller A. Beyond red and blue: what is purple teaming in cyber security? - rehack. *ReHack*. URL: https://rehack.com/cybersecurity/purple-teaming-cyber-security/ (дата звернення: 23.04.2025).

68. What is purple teaming? How can it strengthen security? | redscan. *Redscan*. URL: https://www.redscan.com/news/purple-teaming-can-strengthen-cyber-security/ (дата звернення: 23.04.2025).

69. Mindgard. Breach and attack simulation (BAS) vs. red teaming: what's the difference? - mindgard. *Mindgard - Automated AI Red Teaming & Security Testing*. URL: https://mindgard.ai/blog/breach-and-attack-simulation-vs-red-teaming (дата звернення: 23.04.2025).

70. Cyber security blog - oneconsult AG. *Oneconsult AG*. URL: https://www.oneconsult.com/en/blog/attack-simulation-red-teaming/the-differences-between-penetration-test-and-red-teaming/ (дата звернення: 23.04.2025).

71. Penetration testing or cybersecurity audit: which is right for whom?. *mssolutions*. URL: https://mssolutions.ca/en/blogue/news-en/penetration-testing-or-cybersecurity-audit-which-is-right-for-whom/ (дата звернення: 23.04.2025).

72. Özeren S. Breach and attack simulation vs. red teaming. *Automated Security Validation Platform | Picus*. URL: https://www.picussecurity.com/resource/blog/breach-and-attack-simulation-vs-red-teaming (дата звернення: 23.04.2025).

73. Caldera. *Caldera*. URL: https://caldera.mitre.org/ (дата звернення: 23.04.2025).

74. Welcome to atomic red team. *AtomicRedTeam*. URL: https://www.atomicredteam.io/ (дата звернення: 23.04.2025).

75. The security validation platform. *Automated Security Validation Platform | Picus*. URL: https://www.picussecurity.com (дата звернення: 23.04.2025).

76. Home page. *Cymulate*. URL: https://cymulate.com/ (дата звернення: 23.04.2025).

77. Welcome to pentera. *Pentera*. URL: https://pentera.io/ (дата звернення: 23.04.2025).

78. Січкар Я., Барановська Л. Тестування систем захисту з використанням симуляції кібератак. VIII Міжнародна науково-практична конференція “Проблеми кібербезпеки інформаційно-телекомунікаційних систем” (PCSITS), 11 квітня 2025, Київ, Україна, С. 93-94.

79. The rise of credential compromise attacks | fortinet. *Fortinet*. URL: https://www.fortinet.com/resources/articles/credential-compromise-attacks (дата звернення: 23.04.2025).

80. Home. *GitHub*. URL: https://github.com/redcanaryco/invoke-atomicredteam/wiki (дата звернення: 23.04.2025).

81. We stop breaches with AI-native cybersecurity. *CrowdStrike*. URL: https://www.crowdstrike.com/en-us/ (дата звернення: 23.04.2025).

82. Welcome to MITRE Caldera’s documentation! – caldera documentation. *MITRE Caldera*. URL: https://caldera.readthedocs.io/en/latest/ (дата звернення: 23.04.2025).

83. Red Report 2025. *Automated Security Validation Platform | Picus*. URL: https://www.picussecurity.com/red-report (date of access: 23.04.2025).

84. Labs P. Ukrtelecom's cybersecurity transformation: optimized SIEM rules and rapid threat detection engineering. *Automated Security Validation Platform | Picus*. URL: https://www.picussecurity.com/resource/case-study/ukrtelecom (дата звернення: 23.04.2025).

ДОДАТОК А
СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

Тези наукових доповідей:

1. Січкар Я., Барановська Л. Тестування систем захисту з використанням симуляції кібератак. VIII Міжнародна науково-практична конференція Проблеми кібербезпеки інформаційно-комунікаційних систем" (PCSITS), 11 квітня 2025, Київ, Україна, С. 93-94.

ДОДАТОК Б
ОПИС ТЕХНІК, ЯКІ БУЛИ ВИКОРИСТАНІ ДЛЯ СИМУЛЯЦІЇ КІБЕРАТАК ЗА ДОПОМОГОЮ МОДУЛЮ ATOMICREDTEAM

T1003.001 – OS Credential Dumping: LSASS Memory

Зловмисники можуть спробувати отримати доступ до облікових даних, що зберігаються в пам'яті процесу служби підсистеми Local Security Authority Subsystem Service (LSASS). Після входу користувача в систему система генерує та зберігає різноманітні облікові дані в пам'яті процесу LSASS. Ці облікові дані можуть бути зібрані адміністративним користувачем або SYSTEM і використані для здійснення бічного переміщення за допомогою використання альтернативних засобів автентифікації. Так само, як і в методах з використанням внутрішньої пам'яті, пам'ять процесу LSASS може бути вивантажена з цільового хоста і проаналізована на окремій системі.

T1003.002 – OS Credential Dumping: Security Account Manager (SAM)

Зловмисники можуть отримати доступ до SAM — бази даних, що зберігає локальні облікові дані Windows, включаючи хеші паролів. SAM розміщується в системному реєстрі, а також у вигляді файлу на диску. При отриманні привілеїв адміністратора або SYSTEM, зловмисник може експортувати вміст SAM для подальшого аналізу, зламу хешів або повторного використання автентифікації (наприклад, "pass-the-hash").

T1003.003 – OS Credential Dumping: NTDS

Зловмисники можуть намагатись отримати доступ до файлу ntds.dit на контролері домену, який містить дані Active Directory, зокрема хеші паролів доменних користувачів. Отримання доступу до цього файлу дає змогу зловмиснику здійснити повну компрометацію домену. Часто використовуються інструменти типу ntdsutil, Volume Shadow Copy, або secretsdump.py з пакету Impacket.

T1053.005 – Scheduled Task/Job: Scheduled Task

Зловмисники можуть створити заплановані завдання у Windows, щоб реалізувати автоматичний запуск шкідливого коду. Це дозволяє зловмиснику закріпитись в системі та уникнути виявлення. Завдання можуть бути створені вручну або через командний рядок за допомогою schtasks, PowerShell або сторонніх скриптів, і можуть запускатися від імені користувача або системи.

T1078.003 – Valid Accounts: Local Accounts

Зловмисники можуть використовувати легітимні локальні облікові записи для доступу до системи. Це дозволяє уникати виявлення, оскільки дії здійснюються під справжнім обліковим записом. Цей метод часто застосовується для збереження доступу після компрометації або при розширенні впливу в інфраструктурі.

T1134.004 – Access Token Manipulation: Parent PID Spoofing

Зловмисники можуть змінити ідентифікатор батьківського процесу (PPID), щоб замаскувати походження виконуваного процесу. Це ускладнює виявлення шкідливої активності, оскільки процес виглядає як нащадок легітимного процесу, наприклад explorer.exe. Такі техніки використовуються для уникнення засобів моніторингу та антивірусного ПЗ.

T1543.003 – Create or Modify System Process: Windows Service

Зловмисники можуть створити або змінити Windows-сервіси для уникнення виявлення або підвищення привілеїв. Створені сервіси можуть автоматично запускатися при завантаженні системи, що забезпечує довготривалу присутність. Такі сервіси можуть запускатися від імені SYSTEM або іншого привілейованого користувача.

T1546.008 – Event Triggered Execution: Accessibility Features

Зловмисники можуть змінювати системні ярлики та комбінації (наприклад, Sticky Keys) для запуску командного рядка або іншого коду із екрана входу. Ці функції часто працюють з правами SYSTEM, і заміна їх виконавчих файлів дозволяє обійти автентифікацію, забезпечуючи прямий доступ до системи.

T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

Зловмисники можуть додавати записи в ключі реєстру Run або розміщувати ярлики у папках автозавантаження, щоб їх код виконувався автоматично при вході в систему. Це дозволяє досягти присутності в системі, зберігаючи доступ навіть після перезавантаження.

T1547.004 – Boot or Logon Autostart Execution: Winlogon Helper DLL

Зловмисники можуть модифікувати параметри реєстру Winlogon, зокрема ключі Userinit або Shell, для завантаження додаткових DLL при вході користувача. Такі DLL можуть містити шкідливий код, який буде виконуватися з високими привілеями при кожному вході.

T1548.002 – Abuse Elevation Control Mechanism: Bypass User Account Control

Зловмисники можуть обійти контроль облікових записів користувача (UAC), щоб підвищити свої привілеї без відома користувача. Це дозволяє виконувати дії від імені адміністратора, уникаючи повідомлень безпеки. Існує багато технік обходу UAC, зокрема використання легітимних процесів Windows або зміна ключів реєстру. Такий підхід часто використовується для закріплення та подальшого розгортання шкідливого ПЗ.

T1552.001 – Unsecured Credentials: Credentials In Files

Зловмисники можуть шукати облікові дані у відкритому вигляді в конфігураційних або текстових файлах, які залишені розробниками або адміністраторами. Часто такі дані зустрічаються в скриптах, batch-файлах, конфігураційних файлах додатків. Такі файли можуть бути виявлені через локальний пошук або автоматизовані сканери.

T1552.004 – Unsecured Credentials: Private Keys

Зловмисники можуть шукати приватні ключі (наприклад, SSH) у файловій системі, які не були належним чином захищені. Наявність таких ключів дозволяє зловмиснику отримати доступ до інших систем без паролю.

T1555.003 – Credentials from Password Stores: Credentials from Web Browsers

Зловмисники можуть отримати облікові дані з веб-браузерів, читаючи файли, специфічні для цільового браузера. Веб-браузери зазвичай зберігають облікові дані, такі як імена користувачів і паролі веб-сайтів, щоб їх не потрібно було вводити вручну в майбутньому. Веб-браузери зберігають облікові дані в зашифрованому форматі в сховищі облікових даних; однак існують методи для вилучення облікових даних у відкритому вигляді.

Наприклад, в системах Windows зашифровані облікові дані можна отримати з Google Chrome, прочитавши файл бази даних AppData\Local\Google\Chrome\User Data\Default\Login Data.

T1558.003 – Steal or Forge Kerberos Tickets: Kerberoasting

Зловмисники можуть експортовувати квитки Kerberos для облікових записів, пов’язаних із сервісами, і намагатися їх зламати офлайн. Ці облікові записи часто мають слабкі паролі. Якщо хеш буде розшифрований, зловмисник отримає облікові дані, які можна використати для доступу до критичних сервісів або бічного переміщення.