МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут захисту інформації

На рецензію	До захисту
Доцент кафедри УІКБ	Доцент кафедри УІКБ
кандидат технічних наук, доцент	кандидат технічних наук, доцент
_____С. В. Легомінова	_____ С. В. Легомінова
«___»_____20__ р	«___»_____20__ р

КВАЛІФІКАЦІЙНА РОБОТА

другого магістерського рівня вищої освіти

на тему:

ШЛЯХИ ФОРМУВАННЯ КІБЕРСТІЙКОСТІ ДЛЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА (УСТАНОВИ, ОРГАНІЗАЦІЇ)

СТУДЕНТ: Костроміна Марія Олександрівна _____
(підпис)

КЕРІВНИК: ктн. Рабчун Дмитро Ігорович _____
(підпис)

НОРМОКОНТРОЛЕР: _____ _____
(підпис)

Київ – 2023

Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
Кафедра управління інформаційною та кібернетичною безпекою
Спеціальність 125 Кібербезпека
Спеціалізація Управління інформаційною та кібернитичною безпекою
Другого магістерського рівня вищої освіти

«ЗАТВЕРДЖУЮ»
Завідувач кафедри УІКБ
_____С.В. Легомінова
(підпис)

«___»_____ 20__ р

ЗАВДАННЯ
на дипломну роботу
студентці Костроміній Марії Олександрівні

1. Тема роботи «ШЛЯХИ ФОРМУВАННЯ КІБЕРСТІЙКОСТІ ДЛЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА (УСТАНОВИ, ОРГАНІЗАЦІЇ)», затверджена наказом по університету від «__» _____ 20__ р. №__ .

2. Термін здачі студентом оформленої роботи «__» _____ 20__ р.

3. Об’єкт дослідження: кіберстійкість підприємства.

4. Предмет дослідження: шляхи формування кіберстійкості підприємства (установою, організацією).

5. Мета дослідження: обґрунтування шляхів формування кіберстійкості підприємства (установою, організацією).

6. Перелік питань, які мають бути розглянуті:

6.1. Дослідити теоретичні аспекти поняття кіберстійкості.

6.2. Проаналізувати принцип формування кібестійкості та основні його складові.

6.3. Обґрунтувати шляхи формування кіберстійкості для забезпечення інформаційної безпеки підприємства (установи, організації).

7. Дата видачі завдання «15» вересня 2022 р.

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання: «15» вересня 2022 року

№ з/п	Етапи дипломної роботи	Термін виконання етапів	Примітка
1.	Визначення об’єкту, предмету, мети та завдань досліджень	23.09.2022	
2.	Збір та аналіз літератури	30.09.2022	
3.	Дослідження теоретичних аспектів поняття кіберстійкості	17.10.2022	
4.	Аналіз принципів формування кібестійкості та основних його складових	01.11.2022	
5.	Обґрунтування шляхів формування кіберстійкості для забезпечення інформаційної безпеки підприємства (установи, організації)	15.11.2022	
6.	Формулювання висновків за результатами проведеного дослідження	22.11.2022	
7.	Оформлення роботи	03.01.2023	
8.	Оформлення презентації	04.01.2023	
9.	Отримання рецензії на роботу	05.01.2023	
10.	Захист дипломної роботи в ДЕК	17.01.2023	

Студент: _____ М.О. Костроміна
(підпис)

Науковий керівник: _____ Д. І. Рабчун
(підпис)

РЕФЕРАТ

Дипломна робота присвячена дослідженню шляхів формування кіберстійкості для забезпечення інформаційної безпеки підприємства (установи, організації). Робота складається зі вступу, трьох розділів, що містять 34 рисунка, висновків та списку використаних джерел з 20 найменувань. Загальний обсяг роботи становить 79 аркушів, з яких 2 аркуша займає список використаних джерел.

Об'єкт дослідження – кіберстійкість підприємства (установи, організації).

Мета дослідження: обґрунтування шляхів формування кіберстійкості підприємства (установою, організацією).

Методи дослідження. У роботі використовуються методи порівняння, узагальнення, синтезу та методи системного аналізу шляхів формування кіберстійкості підприємства (установи, організації).

Як результат у роботі розглянуто поняття стійкості, кібербезпеки та кіберстійкості; проведено аналіз, порівняння та зіставлення даних понять; досліджено особливості методів формування кіберстійкості; проаналізовано ключові компоненти, які повинен містити в собі план кіберстійкості та вироблені рекомендації щодо планування та впровадження плану кіберстійкості в інфраструктуру підприємства (установи, організації).

Галузь використання. Розроблені підходи можуть бути використані при плануванні та реалізації концепцій кіберстійкості у контексті протидії загрозам та забезпеченні інформаційної безпеки підприємства (установи, організації).

Ключові слова: СТІЙКІСТЬ, КІБЕРСТІЙКІСТЬ, КІБЕРБЕЗПЕКА, КІБЕРАТАКА, БЕЗПЕРЕРВНІСТЬ, ВІДНОВЛЕННЯ, РИЗИК, ОЦІНКА РИЗИКУ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

- DR (disaster recovery) – аварійне відновлення.
- BCP (business continuity plan) – план безперервності бізнесу.
- EC plan (emergency communications plan) – план аварійної комунікації.
- BCDR (business continuity and disaster recovery) – відділ безперервності бізнесу та аварійного відновлення.
- BIA (business impact analysis) – аналіз впливу на бізнес.
- RA (risk assessment) – оцінка ризику.
- RPO (recovery point objective) – ціль точки відновлення.
- RTO (recovery time objective) – цільовий час відновлення.
- CSO (Chief Security Officer) – директор з безпеки організації.
- COO (Chief Operating Officer) – операційний директор.
- CISO (Chief Information Security Officer) – керівник відділу безпеки.
- NIST – Національний інститут стандартів і технологій.
- EDR (Endpoint detection and response) – виявлення та реагування на загрози на кінцевих точках.
- XDR (Extended detection and response) – Розширене виявлення та відповідь.
- IDS/IPS (Intrusion detection and prevention systems) – Системи виявлення та запобігання вторгненням.
- MDR (Managed detection and response) – Кероване виявлення та реагування.
- NDR (Network detection and response) – Виявлення та відповідь мережі.

ВСТУП

Актуальність теми. За останні роки кількість кібератак та їхній вплив на бізнес значно зросла. Збої в роботі критичних систем компанії можуть призвести до фінансових втрат, зривів бізнесу, шкоди репутації та адміністративної відповідальності. Раннє виявлення та швидке відновлення дозволяють організаціям пом'якшити ризики та наслідки, забезпечуючи безперервність бізнес-процесів.

Непередбачуваність і швидка еволюція потенціалу кіберзагроз роблять зусилля з оцінки ризиків нездатними адекватно вирішити проблеми кібербезпеки критичних систем інфраструктури. З цієї причини традиційний підхід захисту кіберсистем від виявлених загроз виявився неможливим. Єдиним справжнім захистом, який могли б використати фахівці з кібербезпеки, щоб захистити системи від безлічі потенційних кіберзагроз, було б заборонити кіберсистемам доступ до Інтернету.

Подібно до того, як біологічні системи виробляють імунітет, як спосіб реагувати на інфекції, кіберсистеми також повинні пристосовуватися до постійних загроз, які продовжують атакувати життєво важливі функції системи, і вміти віновлюватись після кібератак.

Отже, дана тема є актуальною для вивчення, так як кіберстійкість має вирішальне значення, оскільки вона дозволяє бізнесу продовжувати функціонувати з найменшими збоями в умовах кібератаки.

Мета і завдання дослідження. Мета роботи полягає в обґрунтуванні шляхів формування кіберстійкості підприємства (установою, організацією).

Для досягнення цієї мети в роботі необхідно виконати наступні завдання:

1. Дослідити теоретичні аспекти поняття кіберстійкості.

2. Проаналізувати принцип формування кібестійкості та основні його складові.

3. Обґрунтувати шляхи формування кіберстійкості для забезпечення інформаційної безпеки підприємства (установи, організації).

Об'єкт дослідження – кіберстійкість підприємства.

Предмет дослідження – шляхи формування кіберстійкості підприємства (установою, організацією).

Методи дослідження. Для вирішення зазначеного вище наукового завдання в роботі використані методи методи порівняння, узагальнення, синтезу та методи системного аналізу шляхів формування кіберстійкості підприємства (установою, організацією).

Наукова новизна одержаних результатів. Розроблені підходи можуть бути використані при плануванні та реалізації концепцій кіберстійкості у контексті протидії загрозам та забезпеченні інформаційної безпеки підприємства (установи, організації).

Практичне значення одержаних результатів. Застосування напрацювань дадуть змогу здійснити обґрунтований вибір методів і засобів для побудови і забезпечення кіберстійкості підприємства (установи, організації).

РОЗДІЛ 1
ЗАГАЛЬНА ХАРАКТЕРИСТИКА ПОНЯТТЯ КІБЕРСТІЙКІСТЬ

1.1 Поняття стійкості та бізнес стійкості

Для того щоб краще розібратись в понятті “кіберстійкість” та принципах її побудови, пропоную почати з основ, а саме з розуміння що таке стійкість та бізнес стійкість.

Стійкість – це властивість за значенням стійкий. В академічному тлумачному словнику ми можемо побачити наступні пояснення слова “стійкий”:

1. здатний твердо стояти, триматися, не падаючи, не коливаючись;
2. який довго зберігає і виявляє свої властивості, не піддається руйнуванню, псуванню і т. ін.;
3. для якого характерні стабільність, постійність; сталий;
4. здатний витримати зовнішній вплив, протидіяти чомусь [1].

Тобто стійкість – це здатність протидіяти негативним факторам та зберігати і виявляти свої властивості, не піддаватися псуванню, руйнуванню, незважаючи на зовнішні впливи.

Якщо розглядати стійкість у розрізі бізнесу, то це здатність організації швидко адаптуватися до збоїв, зберігаючи при цьому безперервні бізнес-операції та захищаючи людей, активи та загальний капітал бренду. Стійкість бізнесу виходить за рамки аварійного відновлення (DR) і безперервності бізнесу, пропонуючи стратегії після катастрофи, щоб уникнути дорогих простоїв, захистити вразливі місця та підтримувати бізнес-операції в умовах додаткових неочікуваних негативних зовнішніх впливів [2].

Стійкість бізнесу починається з розуміння того, що бізнес-процеси та робочі процеси мають бути збережені, щоб організації вижили в разі несподіваних подій. Серед важливих проблем планування стійкості бізнесу є людський фактор. Люди повинні бути підготовлені та навчені тому, як реагувати на хаотичну ситуацію.

План стійкості бізнесу іноді називають планом безперервності бізнесу (BCP). Стійкість є результатом різних підходів до готовності, включаючи безперервність бізнесу, аварійне відновлення технологій, управління кризами, управління ризиками та управління інцидентами [2].

План забезпечення безперервності бізнесу — це документ, який містить важливу інформацію, необхідну організації для продовження роботи під час екстрених ситуацій.

BCP визначає основні функції бізнесу та які системи та процеси повинні підтримуватися, і детально описує, як їх підтримувати [3]. Даний план повинен включати будь-які можливі збої в бізнесі.

BCP покриває ризики, зокрема кібератаки, пандемії, стихійні лиха та людські помилки. Масив можливих ризиків робить для організації життєво важливим план забезпечення безперервності бізнесу, щоб зберегти свою репутацію. Належний BCP зменшує ймовірність відключення електроенергії або відключення елементів IT-систем.

Зазвичай IT-адміністратори створюють план безперервності. Однак виконавчий персонал бере участь у процесі, надаючи знання про компанію та бере участь у впровадженні даного плану в роботу. Вони також забезпечують регулярне оновлення плану безперервності.

За словами консультанта з безперервності бізнесу Пола Кірвана, BCP має містити такі елементи [3]:

- вихідні дані на початку плану, включаючи важливу контактну інформацію;
- процес управління переглядом, який описує процедури управління змінами;
- мета і сфера застосування;
- як використовувати план, включаючи вказівки щодо того, коли план буде розпочато;
- інформація про політику безпеки компанії;
- реагування на надзвичайні ситуації та процедури управління;

- покрокові процедури;
- контрольні списки та блок-схеми;
- словник термінів, використаних у плані; і
- графік перегляду, тестування та оновлення плану.

У книзі «Business Continuity and Disaster Recovery Planning for IT Professionals» Сьюзан Снедакер рекомендує поставити такі питання перед побудовою плану безперервності бізнесу:

1. Як би функціонувала організація, якби настільні ПК, ноутбуки, сервери, електронна пошта та доступ до Інтернету були недоступні?
2. Які засоби контролю та управління ризиками існують?
3. Які критичні відносини та залежності від аутсорсингу?
4. Які обхідні шляхи існують під час збою для ключових бізнес-процесів і внутрішніх функцій, таких як людські ресурси?
5. Яка мінімальна кількість персоналу необхідна для роботи центру обробки даних та інших операцій, і які функції вони повинні виконувати?
6. Які ключові навички, знання та досвід необхідні для відновлення?
7. Які критично важливі заходи безпеки чи операційного контролю необхідні, якщо комп’ютерні системи не працюють? [3]

Етапи планування безперервності бізнесу

Життєвий цикл планування безперервності бізнесу містить наступні п’ять кроків (рис. 1.1):

1. Збір та аналіз інформації, включаючи аналіз впливу на бізнес (BIA) та оцінку ризиків (RA);
2. розробка та проектування плану;
3. впровадження;
4. тестування; і
5. підтримка та оновлення [3].

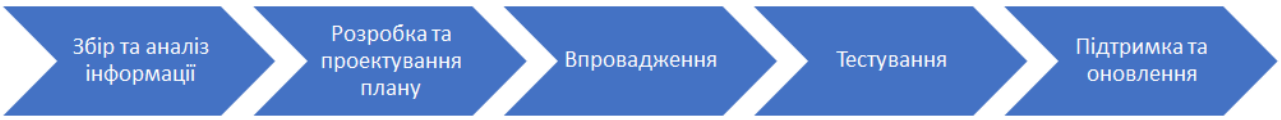

Рис. 1.1 Життєвий цикл плану безперервності бізнесу

Реалізація BCP

Коли компанія розпочала процес планування, вона запускає процеси BIA та RA для збору важливих даних. BIA визначає критичні функції, які повинні виконуватися під час кризи, і ресурси, необхідні для підтримки цих операцій. RA детально описує потенційні внутрішні та зовнішні ризики та загрози, ймовірність їх виникнення та можливу шкоду, яку вони можуть завдати.

Наступний крок визначає найкращі способи боротьби з ризиками та загрозами, викладеними в BIA та RA, а також те, як обмежити шкоду від події. Успішний план безперервності бізнесу визначає покрокові процедури реагування [2].

BCP не має бути надто складним і не має містити сотні сторінок; він повинен містити необхідний обсяг інформації, щоб підтримувати бізнес. Малі підприємства можуть використовувати план на одній сторінці з усіма необхідними деталями. Це може бути більш корисним, ніж довгий план, яким важко користуватися. Ці деталі повинні містити наступне [3]:

- мінімум ресурсів, необхідних для безперервності бізнесу;
- місця, де може відбутися збій критичних бізнес-процесів;
- персонал, необхідний для виконання BCP; і
- потенційні витрати.

Ключові етапи впровадження

Чотири етапи впровадження BCP:

1. Контроль. Необхідно вирішити, хто контролюватиме план. В ідеалі комітет BCP включатиме керівників бізнесу, безпеки та IT.
2. Аналіз. Провести BIA.

3. Подробиці. Необхідно надати відповіді на такі питання щодо безперервності бізнесу, як-от:
    - Хто постраждає від порушення бізнес-процесів?
    - Хто відповідає за збереження копії контактної інформації клієнтів?
    - Як і коли будуть повідомлені клієнти, співробітники та керівництво після збою?
    - Які є альтернативні засоби комунікації, якщо зникне мобільний зв’язок?
    - Які працівники потрібні для відновлення критично важливих бізнес-функцій?
    - На відновленні яких критично важливих активів і послуг компанія повинна зосередитися в першу чергу?
    - Які проблеми необхідно вирішити протягом перших 24-48 годин?
    - Чи кожна команда та відділ має власний BCP? Хто відповідає за план у кожному відділі?
    - Який надзвичайний план наступності для вищого персоналу, включаючи генерального директора?
    - Які працівники будуть виконувати завдання аварійно-відновлювальних робіт?
    - Де відбуватимуться виїзні кризові засідання?
    - Хто взаємодіятиме з місцевими службами реагування на надзвичайні ситуації, такими як пожежники, швидка допомога, поліція та ін.?
    - Хто є ключовими постачальниками, включаючи постачальників резервного копіювання даних? [3]
4. Дія. Створіть BCP, який містить конкретні дії та призначені ролі для кожного етапу надзвичайної ситуації, зокрема:
    - Початкова відповідь. Тобто, як компанія відреагує на збій в роботі протягом перших годин. Це період, коли члени команди зв’язуються та активується BCP.

- Переміщення. На цьому етапі активуються альтернативні можливості.
- Відновлення. Після переміщення персоналу та обладнання починається оцінка збитку та моніторинг відновлення бізнесу. Стратегія відновлення повинна враховувати цільовий час відновлення організації, або RTO, який є максимальним часом, протягом якого IT-системи можуть бути вимкнені після збою, а також цільову точку відновлення, або RPO, що є максимальною втратою даних, яку може допустити організація.
- Реставрація. Персонал повертається на початкове робоче місце або на інше місце. Компанія проводить перевірку інфраструктури, документує інцидент і аналізує отриманий досвід [3].

Тестування плану безперервності бізнесу

Технологія, процеси, персонал і обладнання організації постійно змінюються. Тому регулярне тестування, перегляд та оновлення BCP є критично важливим. Тестування плану має проводитися за допомогою настільних вправ, тестового покрокового виконання плану, практики проведення кризових комунікації та антикризових заходів, щоб перевірити життєздатність плану та побачити, як працівники та керівники реагують на стрес.

Регулярне тестування та технічне обслуговування забезпечують актуальність і точність BCP. Проста перевірка плану безперервності бізнесу може включати його обговорення. Комплексний тест вимагає повного аналізу того, що станеться в разі збою в бізнесі.

Випробування можна спланувати заздалегідь або провести незаплановано, щоб краще імітувати кризову подію. Якщо під час тестування виникають проблеми, план слід відповідним чином виправити на етапі перегляду. Перегляд також включає огляд критичних функцій, описаних у BIA, і ризиків, описаних у RA, а також оновлення плану, якщо це необхідно [3].

План безперервності бізнесу необхідно постійно вдосконалювати; не варто чекати кризи для його оновлення. Співробітники, які беруть участь у плані,

повинні регулярно отримувати оновлення та виконувати тестування щодо впровадження етапів плану безперервності бізнесу [3]. Внутрішній або зовнішній аудит плану забезпечення безперервності бізнесу слід використовувати для оцінки ефективності BCP і виявлення областей, які потребують вдосконалення.

Стійкість бізнесу включає різні елементи загальної стійкості, такі як організаційна стійкість, операційна стійкість, кібер стійкість і стійкість ланцюга поставок. Розширення терміну відображає те, наскільки важливою стала стійкість для підприємств, урядів та інших організацій.

Чому планування стійкості бізнесу є важливим?

Тепер уже недостатньо просто відновити бізнес-операції та критично важливі програми після стихійного лиха, кібератаки чи іншої події. Організації повинні бути готові адаптуватися до змін обставин. Як показала криза COVID-19, компаніям довелося швидко пристосовуватися до мінливого робочого середовища, яке включало підтримку віддаленої роботи та гібридних установок [2].

В 2022 році Україна зіткнулася ще з однією кризою – війна. Це призвело до масових кібератак не тільки на інфраструктуру країни, а також на великий та середній бізнес. Повітряні тривоги, обстріли, планові та аварійні відключення електроенергії – такі реалії реалії сьогодення. Бізнесу, щоб вижити, необхідно вміти швидко пристосовуватись до змін, наприклад, орендувати підвальні приміщення чи офіси з бомбосховищем, які облаштовані альтернативним джерелом електроенергії, щоб можна було працювати незважаючи на відключення електроенергії та забезпечити безпеку співробітникам під час повітряних тривог. А також важливо пам’ятати не тільки про безпеку співробітників, але і про безпеку активів, якими володіє організація.

Організації зобов’язані продовжувати свою діяльність, якщо тільки обставини, як-от злиття, не унеможливлюють це. Акціонери та інші зацікавлені сторони очікують, що бізнес продовжуватиме працювати, незважаючи на ймовірність руйнівної події, яка зашкодить фірмі.

У багатьох випадках повернення до колишніх норм може бути недостатнім; старі методи можуть не відповідати тому, як зараз працює бізнес. Стійкість виходить за рамки суворої безперервності бізнесу та DR, забезпечуючи гнучкість, адаптивність і стійкість, необхідні організаціям для адаптації до довгострокових змін у своїй роботі [2].

Що має включати план стійкості бізнесу?

План стійкості бізнесу включає різні елементи (рис. 1.2). Серед них такі:

1. аналіз впливу на бізнес;
2. оцінка ризику;
3. управління ризиками;
4. тестування та імітація певних ситуацій;
5. план аварійної комунікації;
6. BCP – план безперервності бізнесу;
7. план аварійного відновлення;
8. план реагування на інциденти;
9. план управління надзвичайними ситуаціями.

Кожен із цих компонентів може стояти окремо. Однак разом вони створюють структуру, на основі якої розробляється загальний план стійкості.

Найважливішим аспектом плану стійкості бізнесу є визначення кінцевого стану організації після завершення всіх планів відновлення та процесів відновлення. Легко сказати, що компанія оговталась після інциденту, коли вона відновила роботу. Але чи означає це, що він стійкий? Зрештою, організація повинна визначити, яким має бути її кінцевий стан після інциденту. Щоб досягти цього, він повинен визначити, що є станом стійкості.

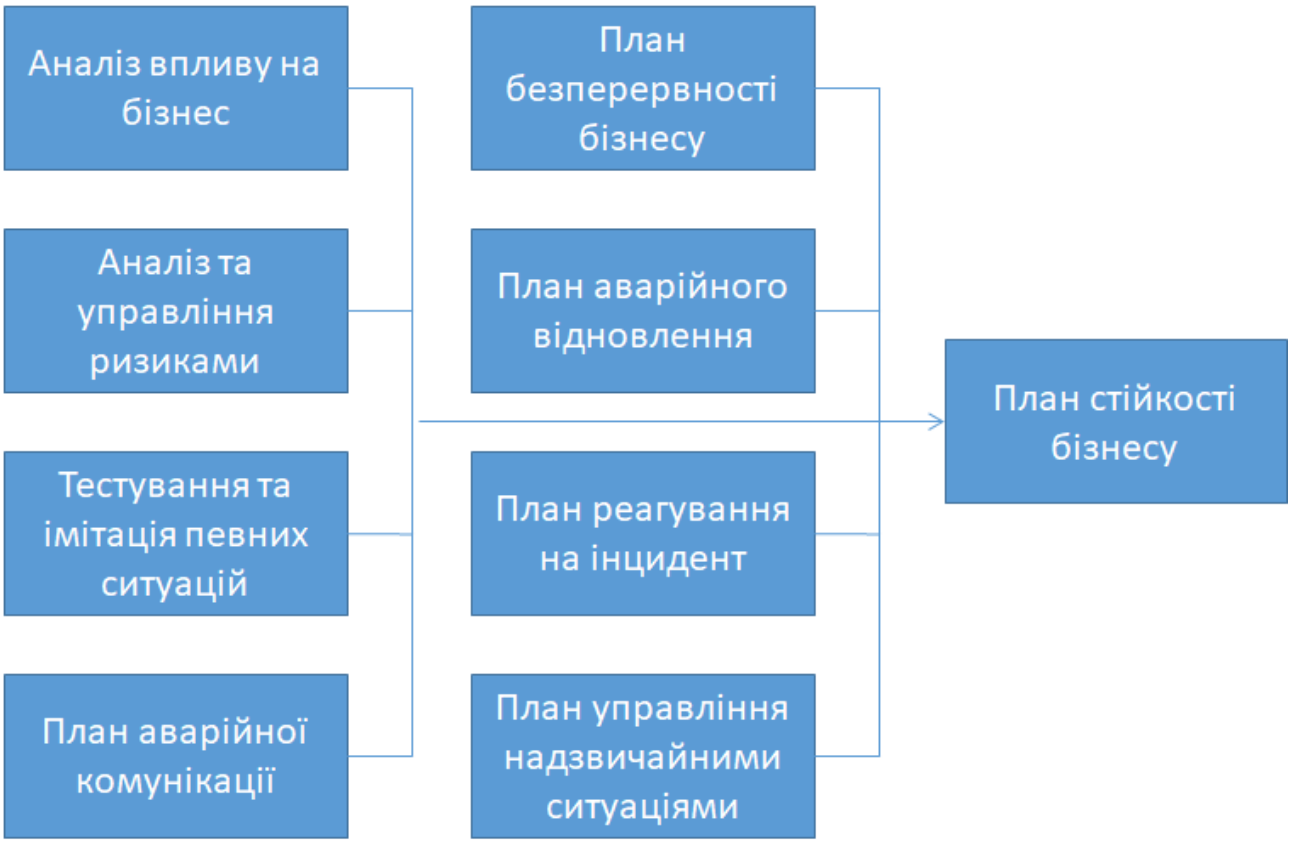

Рис. 1.2 Складові плану по побудові бізнес стійкості

Після події та завершення заходів з реагування безперервність бізнесу та діяльність із ліквідації наслідків відновлення повертають бізнес до роботи. Однак, виходячи з конкретної події та того, як вона впливає на здатність організації вести бізнес, може знадобитися встановити нову або змінити існуючу бізнес-діяльність для нової нормальної діяльності [2]. Це остання частина, де організація демонструє, що має стійкий бізнес (рис. 1.3).

Кроки для побудови плану стійкості бізнесу

План стійкості бізнесу може бути таким же простим, як поєднання управління безперервністю бізнесу, ліквідації та інших планів у план стійкості бізнесу. Швидше за все, багато з цих заходів будуть включені в план стійкості.

Нижче наведено чотири ключові кроки в плані стійкості бізнесу:

1. Визначення, як організація повинна функціонувати після події.
2. Визначення, як він передбачає можливість інциденту та готується до нього.
3. Визначення альтернативних або проміжних методів ведення бізнесу.

4. Визначення впливу культури компанії на відновлення бізнесу.

Поточні стандарти стійкості не мають конкретних рамок для розробки планів стійкості. Вони в першу чергу визначають заходи, які повинні бути частиною цілісного плану.

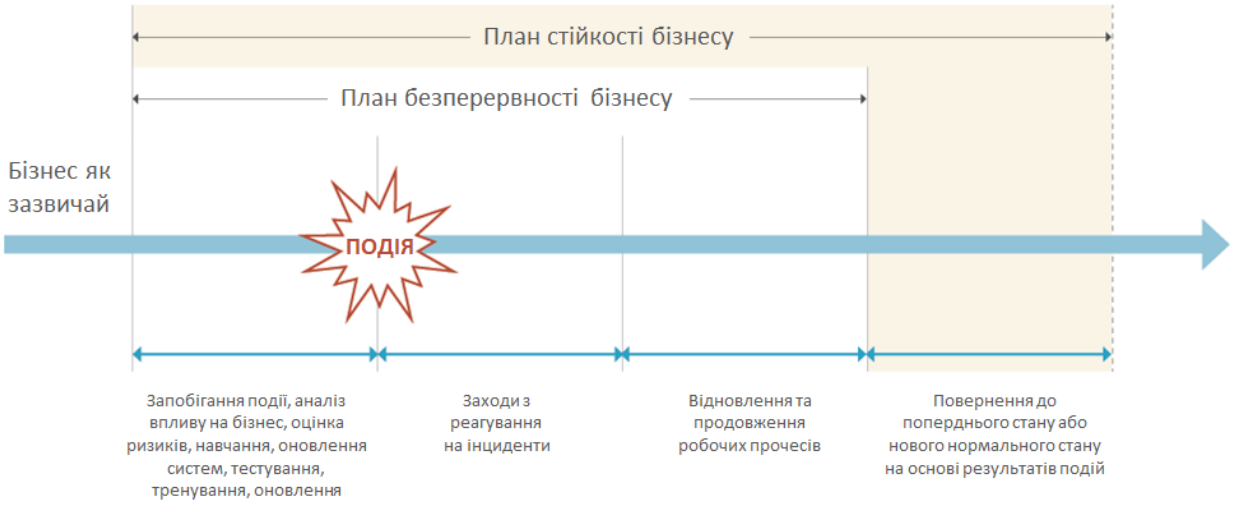

Рис. 1.3 План бізнес стійкості в дії

Хто повинен бути менеджером зі стійкості бізнесу в організації?

Визначення того, хто повинен керувати діяльністю з управління стійкістю бізнесу, було вічним питанням. Деякі організації мають автономні відділи безперервності бізнесу та аварійного відновлення (BCDR). Інші розподіляють прийняття рішень та інші обов'язки між бізнес-лідерами в різних групах і відділах, таких як інформаційні технології, юридичні, кадрові ресурси, вище керівництво, дотримання вимог, управління ризиками, управління надзвичайними ситуаціями та управління об'єктами [2].

Стандарти та рекомендації щодо стійкості бізнесу

Зараз два стандарти визначають стійкість і встановлюють методи її досягнення:

- ASIS SPC.1-2009 розроблено компанією ASIS International і датується 2009 роком. Він називається «Organizational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use. Він використовує ту саму модель системи управління, яку використовують

інші організації зі стандартизації, такі як International Organization for Standardization (ISO) [2].

- ISO 22316:2017 називається «Security and resilience – Organizational resilience – Principles and attributes». ISO 22316:2017 використовує управління ризиками та інші методи для кращого визначення потенційних бізнес-ризиків, загроз і вразливостей до того, як вони виникнуть. Цей стандарт також передбачає необхідність зосередитися на корпоративній культурі як складовій здатності організації підготуватися до руйнівних подій і запобігти їм [2].

1.2 Передумови виникнення концепції кіберстійкості

Термін «кіберстійкість» досі не є популярним у світі інформаційної та навіть кібербезпеки. Активно його почали обговорювати тільки декілька років тому, хоча в світі безпеки він існує вже багато років. Поняття кіберстійкості включає в себе, крім безпеки, ряд завдань і процесів, які відносяться до інформаційних технологій (наприклад, резервування та відновлення після збоїв) і захисту бренду. Причому питання стійкості і безперервності сервісів в цьому понятті відносяться як до самої компанії, так і до зовнішніх підрядників, які надають такі послуги [4].

Передумовою до появи кіберстійкості як напрямки корпоративної кібербезпеки стало прийняття компаніями факту про неминучість кібератаки. Кіберустійкість дозволяє підготуватися до атаки, забезпечує ефективну діяльність і протидію під час атаки, а також знижує можливі наслідки атаки на компанію.

Елементи кіберстійкості в компанії розділяють на кілька основних категорій: управління, права доступу, сегментування, забезпечення цілісності та конфіденційності даних, активне реагування на інциденти, відновлення і координація, скоординований захист компанії [4]. Такий підхід ґрунтується на кращих практиках побудови і управління кібербезпекою в компаніях, зокрема,

на методологіях, затверджених Національним інститутом стандартів і технологій США (NIST) [4]. Кожна категорія представляє собою комплекс процесів, інструментів і контролів, які формують кістяк управління і кіберстійкістю, і кібербезпекою компанії.

Управління кіберстійкістю повністю базується на процесі управління ризиками в компанії в прив'язці до загальної стратегії розвитку бізнесу. Ця категорія включає в себе управління кіберризиками, аудит кіберзахищеності компанії і розробку стратегії кібербезпеки в компанії. Мета даної категорії інструментів і процесів – в зв'язці бізнесу і кібербезпеки, що дозволяє управляти стійкістю компанії з технічної і з бізнесової точки зору. В рамках категорії впроваджуються процеси управління кіберризиками, проводиться зовнішній і внутрішній аудит кіберзахищеності, впроваджуються програми управління обізнаністю співробітників, розробляються і впроваджуються основні політики та інші організаційно-нормативні документи в області кібербезпеки [4].

Права доступу, а вірніше управління правами доступу для забезпечення кіберстійкості, здійснюється відповідно до принципу їх мінімізації. Це означає, що користувачам необхідно надавати мінімально можливий рівень доступу для виконання їх обов'язків і завдань. Управління доступом користувачів – важливий елемент, який відноситься до процесів авторизації, аутентифікації та моніторингу. Мета цієї категорії – в забезпеченні безпеки даних і моніторингу доступу до даних і інформаційних систем в операційній діяльності компанії та під час кібератаки. Впровадження процесів управління доступом включає в себе роботу з рядовими користувачами, а також з користувачами з привілейованим доступом [4]. Для останніх передбачається опрацювання та впровадження додаткових механізмів аутентифікації і контролю.

Третя категорія, сегментування, має на увазі не тільки звичне вже сегментування мережі, а й сегментування архітектури IT і кібербезпеки для забезпечення багаторівневого захисту даних та інформаційних систем. Відповідно до карти кіберризиків і структури бізнес процесів компанії проводиться логічне і фізичне сегментування на рівні інформаційних систем і IT

активів. Проводиться виділення критично важливих систем і їх ізоляція з наступним забезпеченням жорсткого контролю доступу. Важливим елементом залишається і сегментування на мережевому рівні.

Однією з найбільш важливих категорій є активне реагування на інциденти і кібератаки. Побудова таких процесів включає в себе впровадження автоматизованих засобів виявлення та реагування, а також розробку і впровадження процесів управління реагуванням на кібератаки в компанії. Саме впровадження контролів та заходів активного реагування забезпечує оперативне виявлення і реагування на інциденти. Особлива увага в питаннях активного реагування приділяється роботі з персоналом, підготовці співробітників до кібератаки. Необхідно забезпечити високий рівень обізнаності співробітників в питаннях кібербезпеки, а також підтримувати його і актуалізувати їх знання та вміння. Для цього періодично в компанії повинні проводитися кібенавчання, які імітують атаки різної складності і перевіряють «бойову готовність» компанії [4].

Наступна категорія процесів стосується забезпечення цілісності та конфіденційності даних в компанії. Метою цих елементів є зниження шкоди для інформаційних систем і даних в разі інциденту або атаки. Забезпечення конфіденційності та цілісності варіюється від компанії до компанії, а також залежить від того, чи працює компанія з підрядниками, які мають доступ до чутливих даними. Контролі в даній категорії будуються на логічному і фізичному обмеження доступу до даних як в операційній діяльності, так і під час кібератаки або інциденту.

Категорія моніторингу в термінології кіберстійкості – набагато ширше програмних або апаратних засобів, які виконують подібні завдання. Крім них, серед елементів цієї категорії – постійна оцінка всіх процесів і діяльності компанії з точки зору кібербезпеки і кіберстійкості [4]. Сюди входить, наприклад, проведення регулярних сканувань для визначення уразливостей, тестування на проникнення, аудит безпеки аутсорсингу і контроль усунення всіх знайдених загроз і уразливостей в технологіях і в бізнес процесах компанії. Результати такого моніторингу кіберстійкості компанії використовуються для

регулярних оновлень програм обізнаності співробітників та плануванні розвитку кібербезпеки компанії і всього бізнесу.

Категорія відновлення кіберстійкості базується на стандартних процесах відновлення після збоїв і планування безперервності ведення бізнесу (BCP) [4]. Склад контролів і заходів, впроваджуваних в цій категорії, забезпечує резервне копіювання і відновлення даних, інформаційних систем та активів, а також оперативне і аварійне відновлення бізнес процесів і діяльності компанії після інциденту або атаки. Важливим фактором є постійний перегляд і розвиток процесів відновлення відповідно до нових кіберзагроз для конкретної компанії і в цілому в світі.

Найнезрозумілішою, на перший погляд, є категорія скоординованого захисту. Насправді, ця категорія включає в себе елементи всіх категорій і об’єднує їх в єдину стратегію забезпечення кібербезпеки і стійкості. Як правило, в цю категорію відносять забезпечення кіберстрахування компанії, а також залучення зовнішніх фахівців для проведення цифрових розслідувань успішних кібератак на компанію. Координація захисту компанії включає в себе як технічну складову, так і захист компанії в засобах масової інформації і зв’язку з громадськістю, зв’язок з органами влади, антикризове управління та управління всіма цими аспектами. Цю категорію часто виділяють в окрему послугу – «захист бренду», що по суті своїй одне і те ж.

Впровадження та забезпечення кіберстійкості компанії – великий комплексний проект, який вимагає не тільки фінансових вкладень, а й певного рівня зрілості і готовності компанії до нього. Тому, найбільш ефективним підходом до реалізації такого проекту є поступове впровадження елементів кожної категорії у відповідності зі стратегією розвитку бізнесу. Саме в балансі кіберстійкості і цілей бізнесу знаходиться необхідна гнучкість для забезпечення зростання і безпеки компанії [4].

Десять переваг кіберстійкості

1. Блокує загрози від проникнення в системи організації

2. Виводить внутрішні процеси на вищий рівень, залучаючи всю організацію до ролі та важливості безпеки

3. Підвищує загальну безпеку за допомогою стратегій для покращення управління IT, збільшення зусиль із захисту даних, мінімізації впливу стихійних лих і зменшення людської помилки

4. Зосереджує дефіцитні IT-ресурси та ресурси безпеки там, де вони принесуть найбільшу цінність

5. Створює більше довіри в екосистемах клієнтів, партнерів і постачальників

6. Покращує відповідність державним і галузевим нормам

7. Зберігає конфіденційні дані в безпеці

8. Забезпечує безперервність роботи в разі кіберінциденту шляхом мінімізації часу простою

9. Оптимізує повсякденну роботу IT-відділу організації, покращуючи їхню здатність реагувати на загрози та забезпечуючи безперебійну повсякденну роботу

10. Зменшує фінансові втрати та шкоду репутації [5]

Серед аргументів важливості кіберстійкості можна виділити наступні:

● Кількість кібератак та їхній вплив на бізнес значно зросла за останні роки, причому більше половини (58%) малих підприємств повідомили про порушення даних. звіт

● Порушення призводять до фінансових втрат, зривів бізнесу, шкоди репутації та регуляторних заходів. У 2021 році були найвищі середні витрати на витік даних, які зросли з 3,86 мільйона доларів США до 4,24 мільйона доларів США, що є найвищим середнім загальним збитком за 17-річну історію звіту.

● Раннє виявлення та швидке відновлення дозволяють організаціям пом’якшити ризики та наслідки, забезпечуючи безперервну бізнес-операцію.

● Повсюдне підключення розірвало периметри мережі та розповсюдило програми на багатьох хмарних системах, що призвело до збільшення ресурсів IT-безпеки та значного підвищення кіберризиків [5].

Порушення кібербезпеки більше не є питанням «якщо», а «коли».

Стійкість часто плутають з кількома іншими пов'язаними, але різними поняттями. До них належать ризик, надійність і безпека. Оксфордський словник чітко визначив ці поняття. Ризик — це «ситуація, пов'язана з небезпекою, загрозою» [6]. Якщо ризиком керують належним чином, система досягає стану безпеки, тобто «стану відсутності небезпеки або загрози», або надійності, тобто «здатності протистояти або долати несприятливі умови чи суворе тестування.

Безпека, надійність і ризики пов'язані, вони зосереджені на запобіганні деградації системи та підтримці функціональності на прийнятному рівні до та після несприятливої події. Стійкість – це зовсім інше поняття. Оксфорд визначає це як «здатність швидко оговтатися після труднощів» [6]. Таким чином, оцінка стійкості починається з припущення, що система постраждала. У літературі про кіберризик найчастіше визначають кіберризик у термінах, які поєднують у собі ймовірність небажаної події та міру впливу події.

Хоча існує декілька підходів до оцінки ризику, методи, прийняті регуляторними органами США, здебільшого базуються на ризику = загроза x вразливість x модель наслідків. Наприклад, в описі NIST із публікації NIST SP 800-30 (NIST) зазначено: «Ризик — це функція ймовірності того, що певне джерело загрози виявить конкретну потенційну вразливість, і кінцевий вплив цієї несприятливої події на організацію. щоб визначити ймовірність майбутньої несприятливої події, загрози IT-системі повинні бути проаналізовані в поєднанні з потенційними вразливими місцями та засобами контролю, які існують для IT-системи» [6].

Визначення IT-ризику ISO схоже: потенційна можливість того, що дана загроза використає вразливі місця активу або групи активів і тим самим завдасть

шкоди організації. Він вимірюється в термінах поєднання ймовірності виникнення події та її наслідків.

Ключові компоненти кіберризику відносно добре вивчені. Імовірність успішної кібератаки може бути емпірично виміряна та оцінена апріорі з певним ступенем точності на основі відомих характеристик системи або мереж [6]. Кібервплив на систему є темою, для якої розробляються методи оцінки. Оскільки кіберзагрози важко оцінити кількісно, поточні зусилля переходять від кількісного визначення ризику в конкретних одиницях (наприклад, ймовірність відмови) до прийняття рішень на основі ризику з використанням багатокритеріального аналізу рішень [6].

На відміну від концепції стійкості, концепція ризику не дає відповіді на питання про те, наскільки добре система здатна подолати кібератаку, чи як швидко та наскільки повністю система здатна відновитись після кібератаки. Щоразу, коли ризики ідентифікуються та вживаються заходи для зменшення ризику, залишковий ризик все ще залишається. Таким чином, оцінка стійкості та управління нею частково спрямовані на те, щоб усунути відомий, але незмінний ризик, а також підвищити загальну здатність системи реагувати на невідомі або нові загрози. Міцність — ще одне поняття, яке часто плутають із стійкістю. Надійність тісно пов'язана з ризиком. Надійність означає ступінь, до якого система здатна протистояти неочікуваним внутрішнім або зовнішнім загрозам або змінам без погіршення продуктивності системи. Інакше кажучи, припускаючи, що дві системи – A і B – мають однакову продуктивність, надійність системи A є більшою, ніж система B, якщо однаковий неочікуваний вплив на обидві системи залишає систему A з більшою продуктивністю, ніж система B.

У стандарті IEEE «Стійкість визначається як ступінь, до якого система працює правильно за наявності виняткових вхідних даних або стресових умов навколишнього середовища». Подібним чином, «надійний контроль відноситься до керування невідомими установками з невідомою динамікою, що підлягають невідомим збуренням» [6]. Зверніть увагу, що тривалість відновлення зазвичай

залежить від ступеня пошкодження. Також може бути точка, після якої відновлення неможливо.

Отже, існує зв’язок між надійністю (яка визначає, скільки збитків виникає у відповідь на неочікувану збурення) та стійкістю (яка визначає, як швидко система може відновитися після такого пошкодження). Зокрема, система, якій бракує надійності, часто виходить з ладу без можливості відновлення, отже, пропонуючи низьку відмовостійкість. Тому міцність і стійкість слід розуміти разом.

1.3 Поняття кібербезпеки та кіберстійкості і їх порівняння

Як вже згадувалось раніше, стійкість бізнесу включає різні елементи загальної стійкості, такі як організаційна стійкість, операційна стійкість, кібер стійкість і стійкість ланцюга поставок. Тобто поняття бізнес стійкість є більш обширним та включає в себе кіберстійкість.

Щоб більш детально зрозуміти що являє собою кіберстійкість, пропоную пригадати що означає інформаційна та кібернетична безпека і як ці три поняття перегукуються між собою.

Згідно з ISO/IEC 27000 інформаційна безпека – це збереження конфіденційності, цілісності і доступності інформації [7].

Конфіденційність – це властивість інформації, що вона не надається або не розкривається неавторизованим особам, організаціям або процесам [7].

Цілісність – властивість точності і повноти [7].

Доступність – властивість бути доступним і використовуватися на вимогу уповноваженим суб’єктом [7].

Згідно з ISO/IEC 27032 термін кібербезпека визначається як захист конфіденційності, цілісності та доступності даних у кіберпросторі [8].

Кіберпростір – це взаємозалежна мережа інфраструктур інформаційних технологій, яка включає Інтернет, телекомунікаційні мережі, комп’ютерні системи та вбудовані процесори та контролери в критичних галузях [9].

Що таке кібербезпека?

Кібербезпека полягає в захисті від кібератак, які націлені на корпоративні мережі компанії. Щодо кіберстійкості, то експерти визначають її як реакцію компанії після кібератаки та те, як вона відновиться. На цьому етапі кібербезпека та кіберстійкість представлені як дві окремі операції

Кібербезпеку можна оцінити як першу фазу кіберстійкості в тому сенсі, що будь-яка компанія повинна інтегрувати у свою стратегію кіберстійкості етап кібербезпеки [10].

Концепція кібербезпеки базується на ряді різних процесів, пристроїв, технологій, людських операцій і режимів управління, які впроваджуються для забезпечення захисту комп’ютерних мереж, цифрових активів, а також цифрових систем компанії.

Таким чином, заходи кібербезпеки впроваджуються для запобігання доступу хакерів до мережі та комп’ютерних систем компанії. Ці заходи є частиною так званого проактивного плану дій, який може включати такі елементи [10]:

• Впровадженний процес своєчасного оновлення всього програмного забезпечення та операційних систем.

• Встановлення та коректне налаштування антивірусу та десктопних фаєрволів.

• Дотримання всіх стандартів відповідності для забезпечення захисту конфіденційних даних користувачів.

• Забезпечення безпеки служб і пристроїв від численних зловмисних дій, таких як крадіжка або віруси.

• Блокування всіх екранів комп'ютера.

• Підвищення обізнаності та навчання працівників щодо обов’язку забезпечувати безпеку виконання їхніх щоденних завдань.

• Забезпечення фізичної безпеки приміщень компанії.

Завдяки всьому цьому пакету кібербезпеки організації матимуть більш стабільне становище, яке дозволить їй діяти як бар’єр проти зловмисників і запобігати їх спробам проникнути в їх комп’ютерні системи.

Що таке кіберстійкість?

Поняття кіберстійкість не є настільки поширеним та популярним, як кібербезпека. Більш детельно почали вивчати дане питання відносно нещодавно, хоча поняття існує вже багато років.

Кіберстійкість, окрім безпеки, включає в себе ряд процесів та завдань, які відносяться до захисту бренду і інформаційних технологій, наприклад, резервування та відновлення після збоїв та ін. [4].

Передумовою до появи кіберстійкості як напрямку корпоративної кібербезпеки стало прийняття компаніями факту про неминучість кібератаки. Кіберстійкість дозволяє підготуватися до атаки, забезпечує ефективну діяльність і протидію під час атаки, а також знижує можливі наслідки атаки на компанію (рис.1.4) [4].

Зіткнувшись із поширенням кібератак, не всі заходи безпеки є абсолютно безпомилковими. Саме тут кіберстійкість відіграє ключову роль завдяки впровадженню вдосконалених превентивних заходів, щоб максимально мінімізувати негативний вплив кібератак. До них, зокрема, відносяться [10]:

• Розроблено та впроваджено план щодо резервного копіювання в автономному режимі.

• Навчання персоналу щодо питать кібергігієни та поводження з корпоративними даними.

• Розгляд планів відновлення після проблем зі зв’язками з громадськістю, спричинених впливом кібератаки третьої сторони.

• Виконання на регулярній основі вправ із симуляції атак для підвищення готовності бізнесу у разі кібератаки.

• Створенно план безперервності бізнесу.

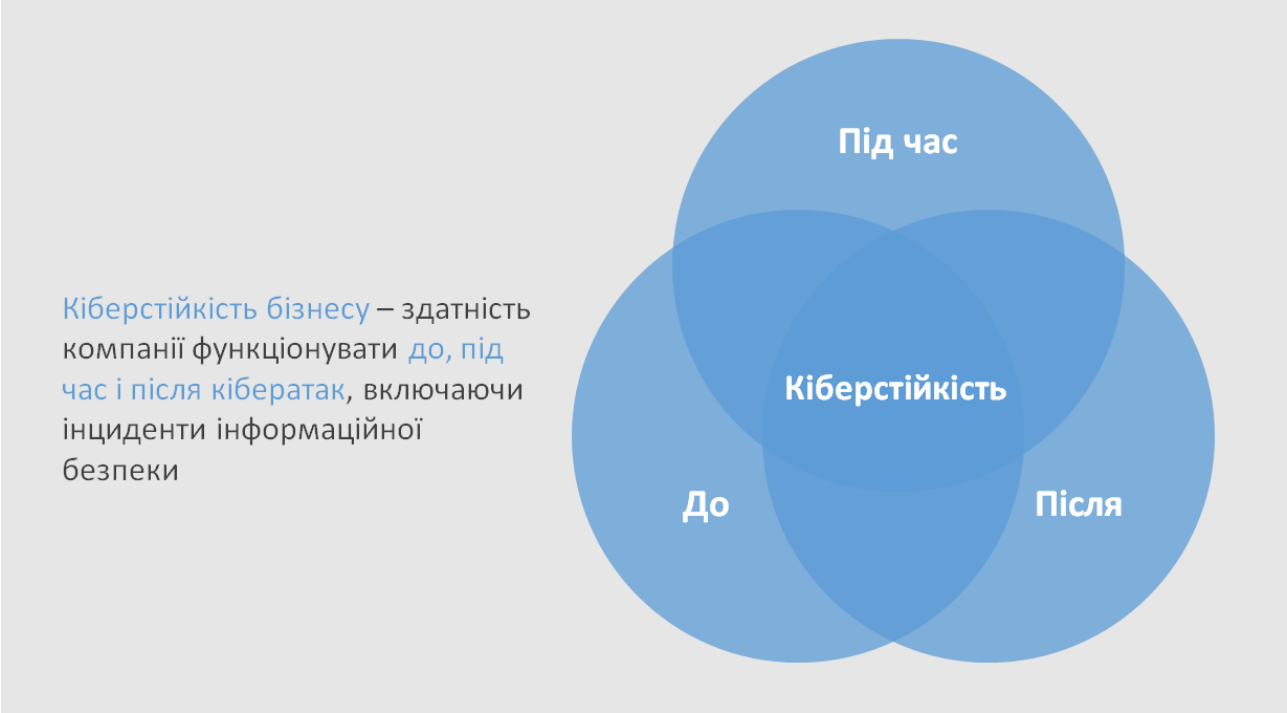

Рис. 1.4 Кіберстійкість бізнесу

Кіберстійкість є важливою та незамінною концепцією для будь-якої організації, оскільки вона дозволяє їй забезпечити оптимальний захист від можливих вразливостей у майбутньому, а також максимально обмежити шкоду та втрати, спричинені кібератаками. До цього додається можливість створення вичерпного звіту про фазу після атаки, що дозволяє краще зрозуміти наслідки кібератаки [10].

Яка різниця між кібербезпекою та кіберстійкістю?

У той час як кібербезпека зосереджується на проактивних діях з метою надання допомоги та підтримки компанії в її боротьбі зі зростаючим поширенням кібератак, таких як програми-вимагачі та шкідливе програмне забезпечення та програми, кіберстійкість, зі свого боку, стосується потенціалу, який може мати компанія щоб максимально обмежити збитки, відновивши роботу у звичному режимі після кібератаки [9]. Крім того, те, що відрізняє кібербезпеку від кіберстійкості, полягає в тому, що перша зосереджена на обмеженні загроз ззовні, тоді як кіберстійкість втручається у зовнішні загрози,

такі як програми-вимагачі, а також у внутрішні загрози, які виникають у формі людської помилки [8].

Які механізми слід прийняти для застосування як для кібербезпеки, так і для кіберстійкості?

Щоб мати можливість легко інтегрувати дві концепції одночасно, а саме кібербезпеку та кіберстійкість, можна застосувати наступні практики [10]:

- Виконання симуляційних тестів: ця практика актуальна в рамках запобігання та, перш за все, підготовки до боротьби з можливою реальною кібератакою. Це дозволяє компанії передбачити дії, які необхідно вжити у випадку атаки, шляхом моделювання інцидентів безпеки, а також дає змогу покращити стратегію кібербезпеки та кіберстійкості компанії.
- Виконання регулярних резервних копій даних та систем: після кібератаки компанія обов’язково має відновити свою нормальну діяльність і за короткий час відновити роботу у звичайному режимі. Для того, щоб досягти цього, дуже важливо, щоб він створював резервні копії своїх даних на регулярній та постійній основі. Звичайно, щоб ці резервні копії були надійними, важливо робити їх в окремій мережі, щоб захистити їх від рук зловмисників. Якби дані були вкрадені або втрачені, компанії було б набагато простіше відновити їх і, отже, ефективніше та швидше забезпечити кіберстійкість.
- Регулярне навчання кібербезпеці та кіберстійкості під час обговорення з радою директорів: належна підготовка всього персоналу в компанії на випадок кібератаки є вирішальним кроком, який необхідно зробити. Співробітники повинні стежити за всіма засобами, що дозволяють захистити дані компанії від потенційних кібератак. Важливо знати, що це стосується всього персоналу, включно з радою директорів, яка найчастіше знаходиться в певному розриві з технічно-технологічними аспектами. Необхідно переконатися, що всі співробітники глибоко розуміють заходи безпеки та знають, як їх застосовувати у разі кібератаки. Обидві концепції, будь то кібербезпека чи кіберстійкість, переслідують одну мету, а саме: захист даних компанії від можливих зловмисних кібератак.

Слід зауважити, що перш ніж приступати до планування кіберзахисту та до планування кіберстійкості, потрібно оцінити вартість активів компанії, так як захист та витрати на стійкість не повинні перевищувати чи дорівнювати вартості активів.

Кіберстійкість проти кібербезпеки

Існує постійна плутанина між кібербезпекою та кіберстійкістю та їхнім взаємозв'язком. Кіберстійкість не є заміною кібербезпеці. Вони доповнюють один одного. Методи кіберстійкості використовуються для підтримки та посилення заходів кібербезпеки [5].

Кібербезпека

Кібербезпека — це оборонна стратегія, яка складається з комбінації технологій і процесів, розроблених для забезпечення виконання політик і захисту систем, мереж, даних та IT-інфраструктури від кіберзагроз (наприклад, зловмисного програмного забезпечення, програм-вимагачів, хакерства, зловмисників) [5]. Ефективна кібербезпека знижує ризик кібератак і захищає ресурси та активи від втрати, крадіжки або пошкодження.

Кіберстійкість

Кіберстійкість поєднує кібербезпеку та операційну стійкість. Це стосується здатності організації постійно запобігати, реагувати, пом'якшувати та успішно відновлюватися після кіберінцидентів. Це включає загрози та атаки з боку кіберзлочинців і зловмисників, а також катастрофічні збої системи через неправильне налаштування та випадкове видалення. Кіберстійкість може бути застосована як до зовнішніх, так і до внутрішніх загроз [5].

Стратегії кіберстійкості припускають, що зловмисники мають перевагу в досягненні своєї мети за допомогою інноваційних інструментів і підходів, використання різних варіантів шкідливого програмного забезпечення та елемента несподіванки. Ця концепція допомагає підприємствам підготуватися, запобігти, реагувати та успішно відновити та відновити свої бізнес-процеси та

бізнес-операції до атаки. Коротше кажучи, кіберстійкість вимагає від бізнесу іншого мислення та більшої гнучкості, щоб передбачати та пом’якшувати атаки.

Бізнес-лідери в усьому світі усвідомлюють, що жодного єдиного рішення для кібербезпеки недостатньо для боротьби з сучасними складними кібератаками, які постійно розвиваються. Незважаючи на посилення захисту, кіберзлочинці все ще можуть скористатися людською помилкою або знайти лазівки та проникнути в мережу та IT-системи вашої компанії. Саме тут використання проактивних інструментів із автоматизацією та штучним інтелектом є ключовим для встановлення кіберстійкості всієї організації [5].

Висновок до розділу 1

У даному розділі було розглянуто теоретичну частину питання, а саме: поняття стійкості, бізнес стійкості та передумови виникнення концепції кіберстійкості. Використовуючи методи порівняння, узагальнення, синтезу та методи системного аналізу порівняно та зіставлено поняття стійкості, кібербезпеки та кіберстійкості; проведено аналіз, досліджено особливості методів формування стійкості бізнесу. Проаналізовано ключові компоненти, які повинен містити в собі план бізнес стійкості.

РОЗДІЛ 2
МЕТОДИ ПОБУДОВИ КІБЕРСТІЙКОСТІ

2.1 Основні складові елементи кіберстійкості

Кіберстійкість – це здатність підприємства обмежити вплив інцидентів безпеки шляхом розгортання й оптимізації відповідних інструментів і процесів безпеки [5]. Кіберстійкість також включає в себе здатність організації постійно зміцнювати свій загальний кіберзахист перед обличчям несприятливих кіберзагроз.

Атрибутами кіберстійкості є (рис. 2.1) [5]:

- Поєднання інформаційної безпеки, безперервності бізнесу та організаційної адаптивності.
- Захист підприємства від негативного впливу внутрішніх і зовнішніх факторів на доступність, цілісність або конфіденційність мережевих IT-систем і пов’язаної інформації та послуг.
- Створення та підтримка груп безпеки, які мають підвищену обізнаність, підвищену пильність і здатні підтримувати безпеку організації.
- Своєчасна підготовка до кіберзагроз, реагування на них і відновлення після них з мінімальними збоями в роботі.
- Здатність адаптуватися до відомих і невідомих криз, загроз, негараздів і викликів.

Рис. 2.1 Атрибути кіберстійкості

NIST визначає кіберстійкість як: здатність передбачати, протистояти, відновлюватися та адаптуватися до несприятливих умов, стресів, атак або компромісів у системах, які використовують кіберресурси або підтримують їх. Кіберстійкість призначена для досягнення місії або бізнес-цілей, які залежать від кіберресурсів, у конкурентному кіберсередовищі [5].

Досягнення кіберстійкості є складним завданням, оскільки підприємствам бракує видимості в реальному часі стану безпеки, пов'язаного з їхніми IT-активами та інфраструктурою, у світлі швидкої еволюції мереж і мінливого середовища загроз. Вони часто не знають, які активи вони повинні захищати, де і як вони можуть бути зламані, а також чи є адекватні засоби контролю безпеки. Якщо засоби контролю є, групи безпеки не впевнені, що вони будуть ефективними проти різних типів загроз. Час – ще один фактор. У більшості випадків служби безпеки не в змозі вчасно реагувати на загрози, оскільки багато процесів виявлення та зменшення ризиків все ще виконуються вручну.

Компоненти стратегії кіберстійкості

Комплексна стратегія кіберстійкості стосується кібербезпеки на всіх рівнях для проактивного захисту організації, виявлення загроз, реагування та відновлення, управління та адаптації [5].

Щоб проактивно захистити системи, програми та дані, на які організація покладається для безперервності бізнесу, стратегія кіберстійкості повинна включати системи кібербезпеки, необхідні для захисту всіх систем, пристроїв, програм і даних. Ключові компоненти стратегії мають включати (рис. 2.2):

- Система управління активами
- Шифрування даних у стані спокою та під час передачі
- Ідентифікація та контроль доступу
- Політика інформаційної безпеки
- Захист від шкідливих програм
- Безпека мережі та комунікацій
- Регулярне оновлення та патчінг систем та додатків
- Фізична та екологічна безпека
- Управління ризиками ланцюга поставок
- Постійне покращення кваліфікацій
- Пошук вразливостей та виявлення загроз [5]

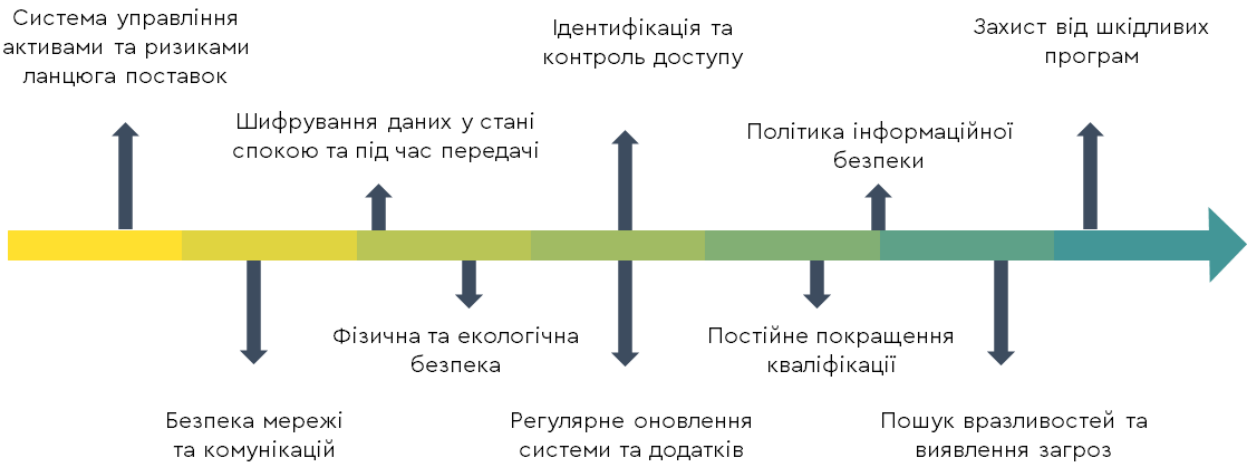

Рис. 2.2 Ключові компоненти стратегії кіберстійкості

Виявлення загроз

Спіймати зловмисників до того, як вони вчинять зловмисний акт, є важливою частиною кіберстійкості. Кілька ключових інструментів, які допомагають у пошуках загрози:

➔ Endpoint detection and response (EDR);
➔ Extended detection and response (XDR);
➔ Intrusion detection and prevention systems (IDS/IPS);
➔ Managed detection and response (MDR);
➔ Network detection and response (NDR) [5].

Відреагувати та відновитись

Імовірність кіберінциденту, незважаючи на найкращу кібербезпеку, залишається високою. Щоб забезпечити безперервність бізнесу, програми кіберстійкості включають:

- Управління безперервністю бізнесу;
- Управління реагуванням на інциденти;
- Управління безперервністю інформаційно-комунікаційних технологій (ІКТ);
- Обмін інформацією та співпраця;
- Security information and event management (SIEM) [5].

Щоб процеси та технології були ефективними в рамках програми кіберстійкості, потрібне управління. Рекомендації щодо підтримки управління для людей, процесів і рішень, які використовуються для підтримки кіберстійкості, включають:

- Залученість на рівні керівництва;
- Зовнішні сертифікації та підтвердження;
- Структура та процеси управління;
- Внутрішні та зовнішні аудити;

- Програма управління ризиками [5].

Адаптуватись

Те, що робить кіберстійкість складною, також сприяє її успіху — постійні зміни. Зміни в ландшафті загроз, поверхні атаки, людях, технологіях і системах – усе це необхідно включати в програми кіберстійкості, коли відбуваються зміни. Ця еволюція гарантує, що організація буде оптимально підготовлена до вирішення будь-яких кіберінцидентів із якомога меншими збоями.

Обґрунтування кіберстійкості

Традиційна оцінка ризиків є привабливою для управління кіберризиками через кількісну природу та єдине значення ризику, яке виводиться. Завдяки цим характеристикам порогові значення ризику легко формалізувати в документах і регулювати на державному рівні [6]. Однак кількісна оцінка ризику зазвичай включає кількісну оцінку ймовірності виникнення події та вразливості до події [11].

Нова кіберреальність та технології представляють нові загрози з невизначеною інтенсивністю та частотою, а вразливі місця та наслідки з точки зору масштабів жертв, економічних втрат, часових затримок чи інших збитків ще не повністю зрозумілі чи змодельовані. У результаті обчислення ризиків стають більш невизначеними та створюють дорогі рішення, оскільки численні, часто гіпотетичні, сценарії загроз можуть вказувати на численні вразливості та катастрофічні збої системи, які неможливо пом’якшити, погасити або відновити. Крім того, користувачі та інші зацікавлені сторони можуть віддавати перевагу погодженню певної втрати продуктивності однієї частини системи порівняно з будь-яким погіршенням іншої частини.

Ключова стратегія управління ризиками полягає у визначенні критичних компонентів системи, які є вразливими до збоїв, і подальшому їх зміцненні [6]. Цей підхід може бути прийнятним для багатьох ізольованих кіберсистем, але коли природа загрози невідома, як обговорювалося вище, важко ідентифікувати всі критичні компоненти, і стає все дорожче діяти консервативно, щоб посилити

або захистити всі частини система проти всіх типів загроз (рис. 2.3). Результатом стала стагнація інвестицій. Оскільки плани пом’якшення ризиків стають дорожчими та відкладаються на час пошуку фінансування, інфраструктура та суспільні системи в основному залишаються неготовими до нових та невизначених загроз.

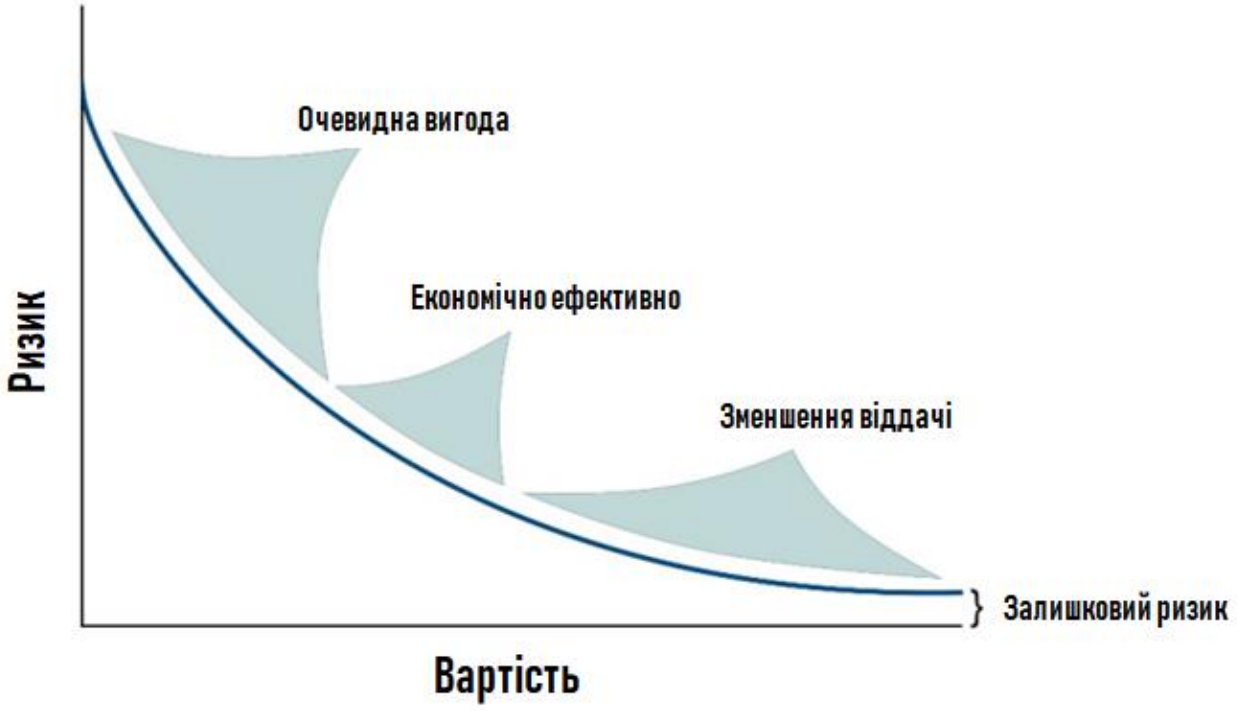

Рис. 2.3 Концептуальна діаграма вартості ризику

Крім того, в обмін на те, щоб прийняти поточні рівні ризику, а не вимагати більших профілактичних і захисних заходів, фінансування можна перерозподілити на зусилля з підвищення стійкості. Для систем, які вже виконали економічно ефективні заходи зі зниження ризику, показано на рис. 2.4 фінансування, яке можна перерозподілити на стійкість шляхом прийняття рівня ризику (a) над рівнем ризику (b) [6]. Паралельно з цими громадськими змінами слід закликати наукове співтовариство розробити моделі прийняття рішень, які визначають оптимальні інвестиції в зниження ризику порівняно з підвищенням стійкості та відновлення.

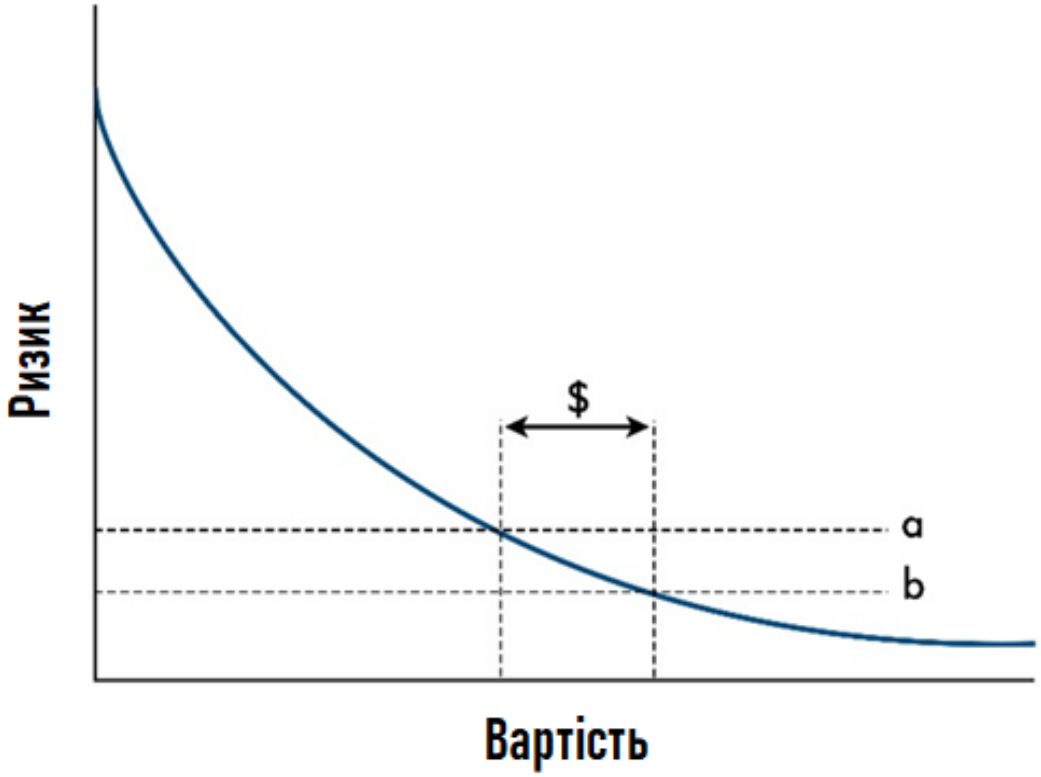

Рис. 2.4 Економічно ефективні заходи зі зниження ризику \12\

2.2 Концепції забезпечення кіберстійкості

Ключові кроки для покращення кіберстійкості

Кіберстійкість — це не монолітне оновлення. Вона складається з кількох кроків із багатьма ітераціями [5]. Нижче пропоную можливий перелік кроків, які організація може вжити для покращення кіберстійкості.

1. Організація видимості в усьому IT-середовищі компанії
2. Донесення стратегії кіберстійкості до рівня керівництва
3. Наймання та утримання професіоналів
4. Зосередитись на основах кібербезпеки
5. Бути проактивним у своїй стратегії кіберстійкості

Організація видимості в усьому IT-середовищі компанії

Першим кроком до кіберстійкості є наявність видимості стану кібербезпеки організації, яка починається з ідентифікації всіх IT-активів,

пов’язаних з організацією, і визначення того, які ІТ-активи знаходяться під загрозою. Це включає наявність бізнес-контексту щодо цих активів, а також будь-яких пов’язаних із ними вразливостей і ризиків. Інформаційні панелі кількісної оцінки кіберризиків дають змогу побачити ризики організації в грошовому еквіваленті. Це дозволяє зацікавленим сторонам визначати пріоритетність дій із зменшення ризиків на основі впливу на бізнес [12]. Інформаційні панелі також забезпечують видимість ефективності засобів контролю безпеки.

Донесення стратегії кіберстійкості до рівня керівництва

Як і у випадку з кібербезпекою, кіберстійкість вимагає значних інвестицій в технології та людей. Ознайомлення ради директорів організації з ризиками злому та кіберстійкості допомагає отримати їхню підтримку для досягнення загальної мети та бюджету, необхідного для зменшення ризику злому шляхом підвищення кіберстійкості. Рекомендовано регулярно інформувати їх, як і виконавчу команду, про те, як дії групи безпеки призводять до зниження бізнес-ризику та як різні проекти безпеки пов’язані з цілями компанії [5].

Наймання та утримання професіоналів

Вирішення організаційних проблем, таких як нестача спеціалістів із безпеки для підтримки операційної та технічної діяльності, є ключовою проблемою, яка може кинути виклик CISO. Спосіб пом’якшити це – задіяти наявні таланти, розвиваючи бажані навички безпеки. Це включає надання їм правильних інструментів, наприклад тих, які використовують автоматизацію та машинне навчання, а також співпрацю з постачальниками, які можуть служити надійними порадниками. Це також означає витратити час на підвищення рівня задоволеності працівників, щоб забезпечити цінні ресурси, які організація вже зберегла.

Зосередитись на основах кібербезпеки

Дотримуйтесь найкращих практик і використовуйте переваги систем та інструментів безпеки, як-от:

- Проактивна безпека
    - Захист від шкідливих програм;
    - Антивірус;
    - Безпека електронної пошти;
    - Захист кінцевої точки, безпека кінцевої точки;
    - Захист від програм-вимагачів;
    - Управління вразливістю на основі ризиків;
    - Єдина інвентаризація активів;
    - Фільтрування URL-адрес [5].
- Профілактична безпека
    - Резервне копіювання;
    - Навчання;
    - Шифрування [5].
- Системи управління безпекою
    - Data Loss Prevention (DLP);
    - Identity access management (IAM);
    - Multi-factor authentication (MFA);
    - Інструменти керування виправленнями;
    - Security information and event management (SIEM) [5].

Бути проактивним у своїй стратегії кіберстійкості

У поточному складному середовищі загроз традиційні тактики безпеки, які здебільшого полягають у реактивному блокуванні та виправленні, є недостатніми. Загальноприйнятий погляд на ідентифікацію та додавання більшої кількості точкових продуктів до набору інструментів став менш ефективним, ніж будь-коли. Перевантаженим і неукомплектованим командам безпеки регулярно доводиться одночасно аналізувати сповіщення, відстежувати вразливості, застосовувати політики безпеки в різних системах і кінцевих точках і точно оцінювати глобальні дані про загрози, щоб з’ясувати, як вони можуть вплинути на них у реальному часі [5].

Щоб впоратися з цими конкуруючими проблемами, організації повинні змінити свою позицію безпеки від суто оборонної та реактивної позиції, зосередженої на зловмисному програмному забезпеченні, до більш проактивного підходу прогнозування та пом'якшення порушень, що покращить як кібер-стійкість, так і продуктивність команди безпеки (рис. 2.5).

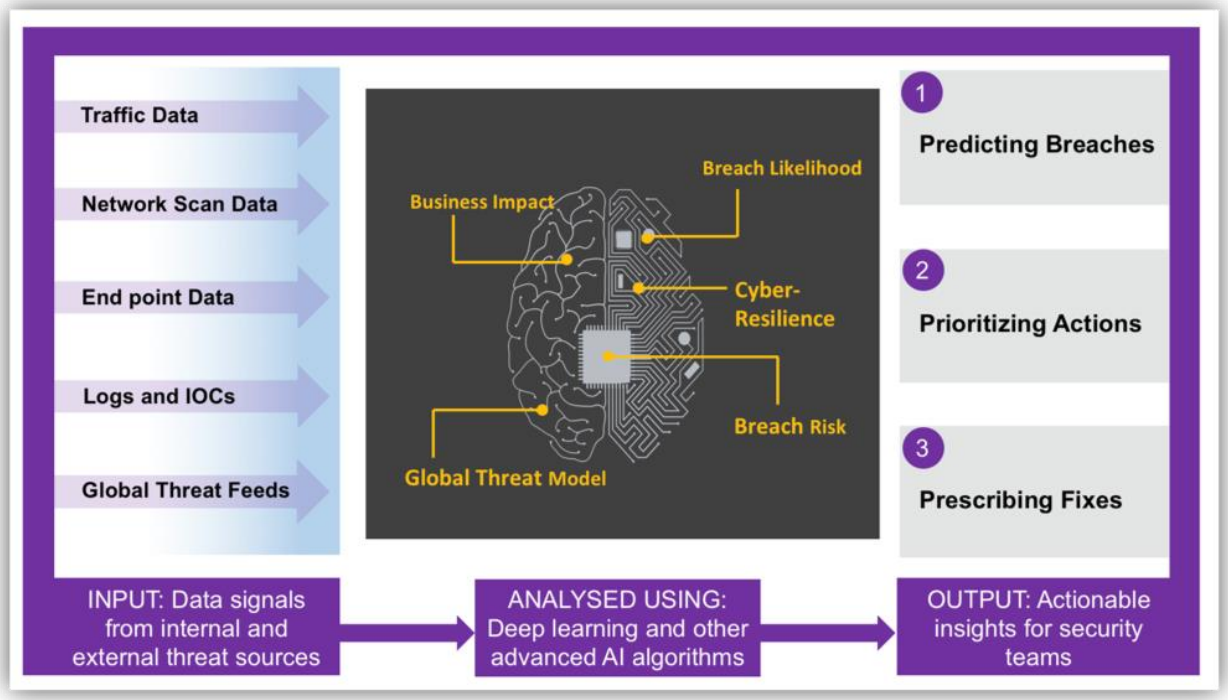

Рис. 2.5 Проактивний підхід прогнозування та пом'якшення порушень [5]

Стійкість і відповідні властивості систем

Кіберстійкість відноситься до здатності системи відновлювати або регенерувати свою продуктивність після того, як кібератаки викликають погіршення її продуктивності (рис 2.6). Наразі, поки ми не заглибимося в показники кіберстійкості, ми можемо сказати наступне: якщо припустити, що дві однаково продуктивні системи A і B зазнали впливу (в результаті кібератаки), який залишив обидві системи з рівним зниженням продуктивності, стійкість системи A є більшою, якщо після певного періоду T вона відновлюється до вищого рівня продуктивності, ніж у системи B [6].

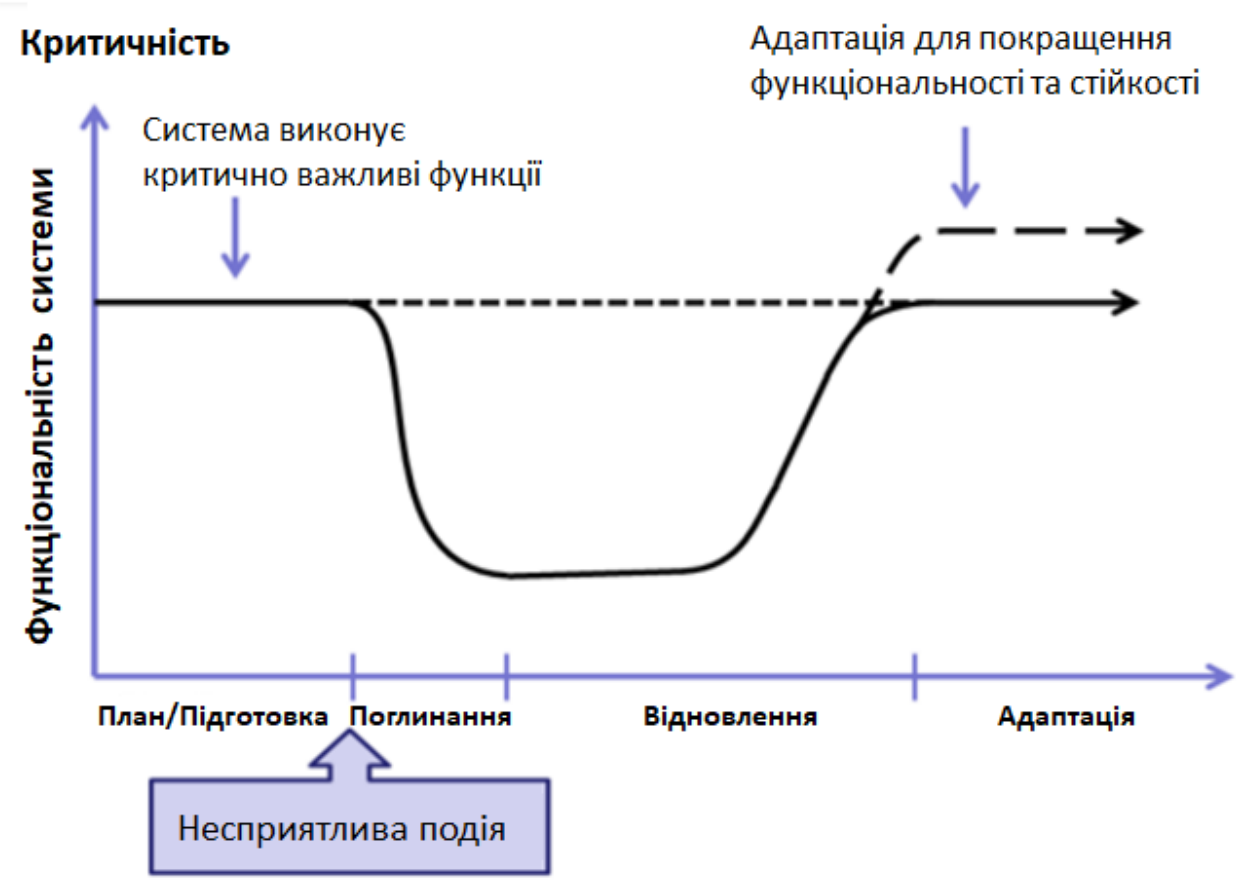

Рис. 2.6 Здатність системи відновлювати або регенерувати свою продуктивність

2.3 Методика впровадження плану з кіберстійкості

Грунтуючись на принципах побудови бізнес стійкості, розглянемо методики побудови кіберстійкості (рис 2.7).

1. Організація видимості у реальному часі.

Існує твердження, яке ви, мабуть, вже чули: неможливо покращити те, що ви не можете виміряти [12]. Крок 1 для покращення кібер-стійкості вашого підприємства – це встановлення системи, яка виявлятиме й аналізуватиме поверхню атак вашого підприємства постійно й комплексно, а також розраховуватиме стійкість. Враховуючи розмір і складність корпоративної поверхні атаки, це завдання вимагає серйозної роботи. Для організації з тисячею співробітників існує понад 10 мільйонів змінних у часі сигналів, які необхідно проаналізувати, щоб точно передбачити ризик порушення [12].

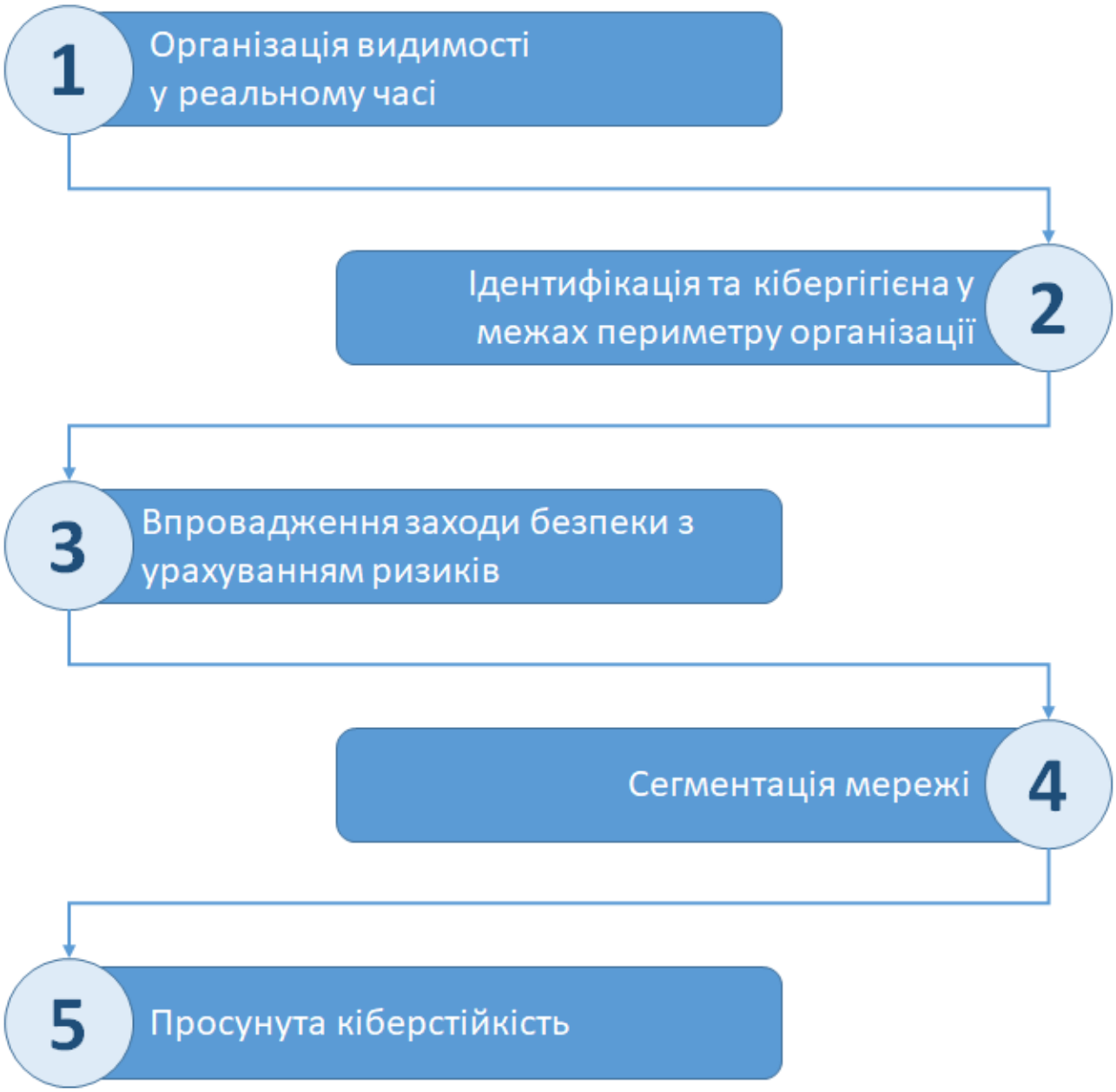

рис. 2.7 План впровадження кіберстійкості

Для організацій із 100 тисячами співробітників нам потрібно включити понад 100 мільярдів сигналів у розрахунок ризику [12]. Запуск сканування Nessus або проходження тесту на проникнення не дадуть компанії необхідної видимості. Застарілі методи охоплюють менше 5% поверхні атаки та не обчислюють математично обґрунтованих показників ризику чи стійкості [12]. Ви також не можете кинути на це завдання армію людей – у них елементарно не вистачить на все це часу. Тому компаніям потрібні спеціалізовані системи, які

здатні виконувати цей масштаб спостереження, аналізу та розрахунку ризику злому та кіберстійкості.

2. Ідентифікація та кібергігієна у межах периметру організації. На кроці 2 ми зосереджуємося на двох речах: надійних механізмах для ідентифікації людей, пристроїв і програм на підприємстві (надійна ідентифікація) і проблемах із станом кібербезпеки у ваших системах, що виходять в Інтернет [12].

Мета надійної ідентифікації користувача полягає саме в здатності ідентифікувати користувачів, які намагаються отримати доступ до певного корпоративного ресурсу чи програми надійним способом. Ідея надійності тут полягає в тому, щоб зробити систему ідентифікації важкою для компроментації, навіть якщо зловмисник вгадав або вкрав паролі користувачів або отримав доступ до пристрою, або зміг перехопити комунікацію [12].

Принцип надійної ідентифікації користувача має також враховувати практичні міркування, такі як той факт, що ваші користувачі отримають доступ до керованих і некерованих програм, а деякі програми/послуги не підтримують такі механізми, як двофакторна автентифікація. Компанії не можуть прикидатися, що ці «важкокеровані» застарілі або тіньові IT-програми не існують або вписуються у чисту канонічну керовану IT-архітектуру.

Практично надійну ідентифікацію користувача можна встановити за допомогою корпоративного продукту Identity and Access Management (IAM), такого як Okta або Cisco Duo, у поєднанні з менеджером паролів, таким як 1password чи KeePass. Це забезпечить надійну багатофакторну автентифікацію та контроль політики, де це можливо, і забезпечить надійну гігієну паролів для керованих і некерованих програм.

Надійну ідентифікацію пристрою можна встановити за допомогою сертифікатів на стороні клієнта, а надійну ідентифікацію програми можна встановити за допомогою сертифікатів на стороні сервера [12]. Керування сертифікатами вимагає певної роботи, і дуже прикро, що більшість організацій не приділяють цьому належної уваги. Необхідно запровадити механізми для

оновлення сертифікатів, термін дії яких закінчується, а також ідентифікації та навчання користувачів, які ігнорують попередження про сертифікати.

Те, що система знаходиться за мережевим екраном, не означає, що компанії можуть недбало ставитися до її захисту.

Кібергігієна розширеного периметра: ваші активи, пов'язані з Інтернетом, є «нульовою точкою», де починаються кібератаки. На кроці 1 вище ми отримали знання про проблеми з кібербезпекою, пов'язані з пристроями, користувачами та додатками на вашому розширеному периметрі. Типові приклади включають невиправлені системи, відсутні паролі або паролі за замовчуванням, відкриті порти, проблеми з конфігурацією безпеки, користувачів, яких можна обманути, не дійсні сертифікати, привілейовані користувачі або важливі користувачі з поганою кібергігієною тощо [12]. Необхідно визначити які з цих проблем є в компанії, шляхом зовнішнього або внутрішнього аудиту, використовуючи відповідні засоби пом'якшення, включаючи зміну конфігурації, виправлення, розгортання елементів керування для захисту кінцевих точок і захисту від фішингу, навчання користувачів фішингу тощо. Ви також повинні подумати про те, як ваші виправлення залишатимуться на місці, тобто як ви будете підтримувати стан кібербезпеки для вашого розширеного периметру з часом.

Недостатньо просто виявити вразливі місця. Компаніям потрібна система, яка автоматично призначає відповідального для кожної вразливості, а потім реєструє їх, відстежує та виявляє за потреби.

3. Поліпшення кібергігієни основних систем; впроваджувати операції безпеки з урахуванням ризиків. На кроці 3 пропоную зосередитись на трьох сферах: покращенні стану кібербезпеки для ваших пристроїв, не пов'язаних з Інтернетом (основна гігієна), запровадженні управління вразливістю на основі ризиків і автоматизованому реагуванні на випадки, що враховують ризики. Кібергігієна основних систем [12].

Покращення кібергігієни основних систем, які за визначенням не є вихідними в Інтернет, має подвійний характер. По-перше, навіть незважаючи на те, що ці системи знаходяться за мережевим екраном, досить ймовірно, що

якийсь пристрій на вашому розширеному периметрі буде скомпрометовано в певний момент часу. Крім того, ми не хочемо, щоб супротивник міг швидко атакувати та скомпрометувати цінну основну систему, яка не захищена належним чином. Важлива реальність, яку слід розуміти: те, що система захищена фаєрволом, не означає, що ми можемо недбало ставитися до її захисту.

Основну кібергігієну можна покращити за допомогою механізмів, подібних до тих, які використовуються для покращення стану кібербезпеки свого периметра. Управління вразливістю на основі ризиків: важливо тримати системи та додатки оновленими та пропатченими. Однак ландшафт загроз постійно змінюється завдяки виявленню нових уразливостей, створенню експлойтів і постійним змінам на підприємстві щодо пристроїв, програм, користувачів, конфігурації та поведінки, що призводить до появи нових вразливостей [12].

Управління вразливістю на основі ризиків – це процес постійного виявлення та пом’якшення вразливостей у всіх ваших активах і всіх векторах атак у пріоритетному порядку на основі ризику. Пріоритезація вразливостей на основі ризиків дуже важлива, оскільки в іншому випадку кількість проблем стане занадто великою для ефективного усунення. Сьогодні сучасне впровадження управління вразливістю на основі оцінки ризику (рис. 2.8) враховуватиме загрози, вплив, компенсаційні засоби контролю та критичність для бізнесу, щоб визначити пріоритетність вразливостей.

Як відомо, недостатньо просто виявити вразливі місця. Їх потрібно виправити. Вам потрібна система, яка призначає відповідальних для кожної вразливості, а потім генерує пріоритетні заявки, що містять увесь відповідний контекст, і призначає їх цим власникам. Звичайно, деякі квитки вимагатимуть тактичних заходів пом’якшення, тоді як інші обов’язкові дії відповідають стратегічним проектам. Усюди, де це можливо, необхідно автоматизувати ці необхідні дії, особливо для проблем, які виникатимуть неодноразово, наприклад, встановлення патчів Windows.

Компаніям також потрібно відстежувати прогрес і повідомляти про це відповідним зацікавленим сторонам. Це вкрай важливо, щоб зацікавлені сторони

за межами команди безпеки зробили внесок у підвищення кіберстійкості. Сучасні системи, такі як Balbix, виводять це на наступний рівень, спрощують процес безперервного управління вразливістю та трансформації кібербезпеки для підприємства, з CISO та CIO [12].

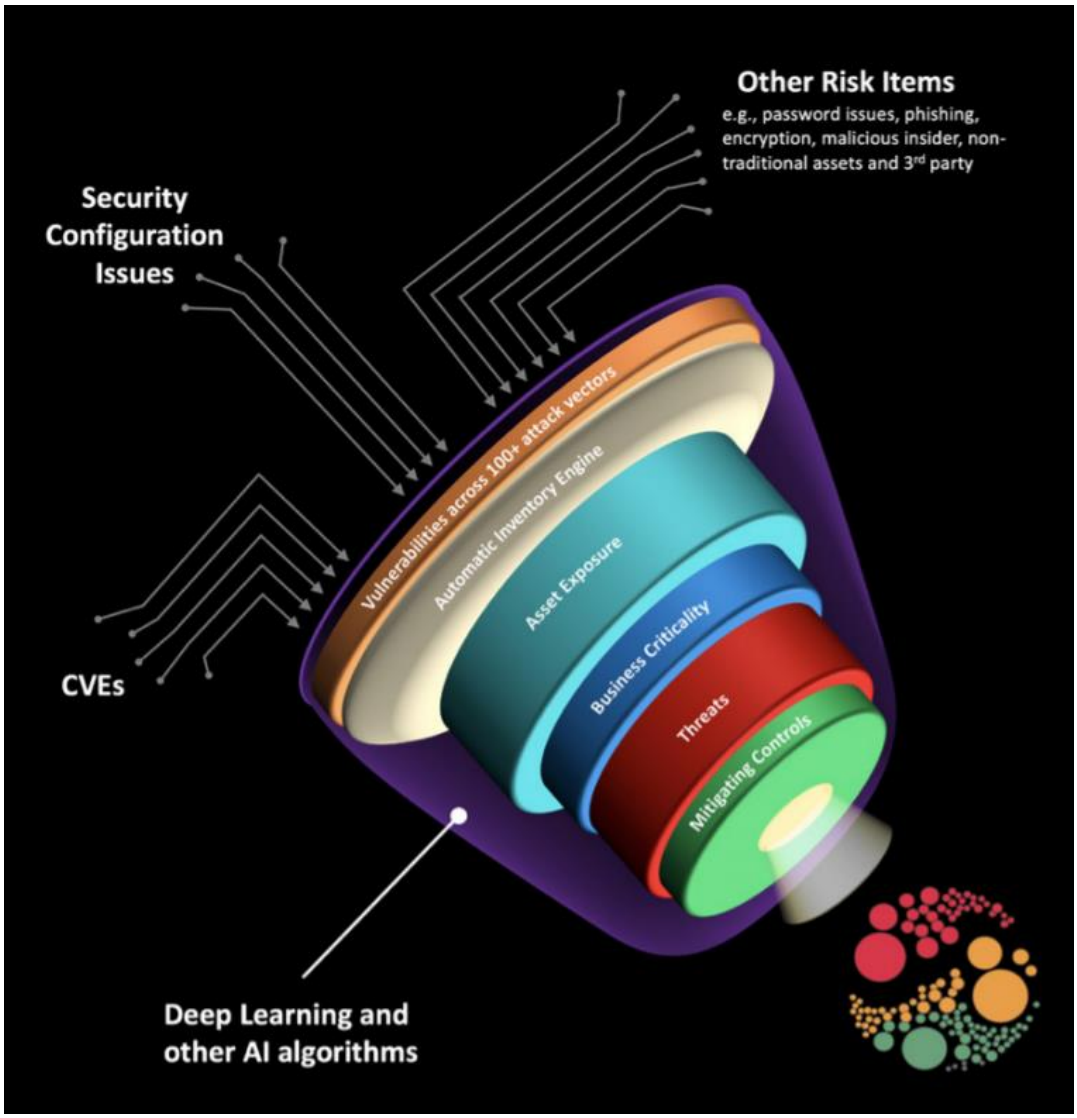

Рис. 2.8 Управління вразливістю на основі ризиків [12]

Автоматизоване реагування на події з урахуванням ризиків: SOC є центром можливостей моніторингу в реальному часі та реагування на події безпеки [14]. Головне завдання — мати справу з обсягом даних про події безпеки з усіх активів підприємства, які ефективно потрапляють у послідовність аналізу, але не пропускають важливі події. Такі інструменти, як SIEM, є першим механізмом фільтрації/зіставлення, але вони сильно обмежені тим, що ви можете зробити [12].

Глибоке навчання та інші передові методи ШІ можуть безперервно аналізувати від 10 до 100 мільйонів точок даних, щоб імітувати знання експертів-аналітиків і детективні методи [12]. Це може підвищити ефективність вашого SOC шляхом визначення пріоритетів діяльності на основі ризику та надання глибокого контексту для аналітиків і інструментів автоматизації. Звичайно, ви повинні автоматизувати якомога більше, і інструменти SOAR роблять це можливим.

4. Динамічна сегментація мережі. Після виконання кроків 1-3 щодо покращення кіберстійкості ви готові взятися за завдання модуляції контролю доступу на мережевому рівні для вашої розширеної мережі [12].

Теорія, що лежить в основі сегментації мережі, полягає в тому, що зловмисник не може (практично) атакувати систему, до якої він не може спрямувати пакети, навіть якщо ця система має деякі вразливості. Сегментація мережі еквівалентна створенню віртуального повітряного проміжку між більш відкритими системами периметра та цінними критично важливими системами. Наприклад, теоретично ви можете налаштувати конфігурацію DHCP так, щоб ноутбуки та настільні комп’ютери ваших привілейованих користувачів отримували IP-адреси в певній VLAN, тоді як усі інші кінцеві точки клієнта отримували адреси DHCP в інших VLAN. Ви також можете налаштувати свої сервери на іншу VLAN і налаштувати мережевий екран/правила переадресації у вашій мережевій інфраструктурі так, щоб адміністративні порти ваших серверів, наприклад RDP і SSH, могли маршрутизуватися лише з VLAN привілейованих користувачів [12]. Усі інші VLAN не можуть надсилати пакети на ці порти будь-якого пристрою в сегменті сервера. Ви також можете заборонити пристроям у VLAN сервера створювати вихідні з’єднання. Це приклади сегментації північ-південь.

Подібним чином ви також можете модулювати трафік зі схід-захід у центрі обробки даних, щоб запобігти боковому переміщенню противника між вашими основними системами.

Системи сегментації мережі третього покоління, що з’являються, надають можливість самонавчання сучасних алгоритмів ШІ для вирішення завдань динамічної сегментації мережі. За допомогою таких систем можна організувати пересилання трафіку таким чином, що а) лише авторизовані строго ідентифіковані користувачі та пристрої можуть направляти пакети до певних систем, і б) лише якщо ризик такого трафіку є нижчим за прийнятний рівень. Це показано на рис. 2.9 [15].

Рис. 2.9 Динамічне сегментування мережі з урахуванням ризиків

5. Розширена кіберстійкість. На кроці 5 ми можемо вивести концепцію динамічної сегментації мережі на наступний рівень. Наприклад, ви можете налаштувати рішення сегментації мережі 3-го покоління таким чином, щоб ваші сервери в AWS або у вашому центрі обробки даних були доступні з клієнтського пристрою, лише якщо пристрій має певний клас сертифіката 802.1x, його користувач пройшов повну Okta перевірити протягом останніх 2 хвилин, пристрій фізично знаходиться в певній географічній зоні (як вимірюється 2-3 методами), пристрій повністю виправлено та відповідає певним вимогам конфігурації безпеки, користувач має правильну поведінку в кібербезпеці — не пішов на веб-сайти з поганою репутацією або клацання минулих пошкоджених сертифікатів за останній час тощо [12].

Загальна форма цього обчислення показана на рис. 2.10. Перш ніж будь-який IP-пакет буде перенаправлено на хост, ми можемо виконати обчислення ризику на основі, а потім на основі результатів обчислення та політики дозволити пакету пройти, відкинути його, утримати пакет, поки ми виконуємо позасмугову повторну автентифікацію, або пересилаємо пакет до приманки чи мережі підробок [16].

Рис. 2.10 Пересилання пакетів на основі ризиків і керування сеансами

Висновок до розділу 2

Більшість організацій розглядають кіберризик як складну технічну проблему, якою має керувати виключно команда безпеки. На жаль, це поняття не може бути далеким від істини, і кіберстійкість може бути реалізована лише за умови співпраці всіх зацікавлених сторін у бізнесі. Найкращий спосіб позбутися організаційних розривів і пояснити бізнесу, що кіберризики є відповідальністю кожного, це надати кожному можливість брати участь в управлінні ризиками. Від IT до інженерів, від C-suite до всіх співробітників, від ваших партнерів до сторонніх постачальників – кожен має усвідомити, що безпека – це питання бізнесу, а не лише технологічна проблема. Усі організаційні підрозділи мають бути обізнаними та виконувати свою роль у забезпеченні загальної кібербезпеки.

РОЗДІЛ 3
РІШЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІЗ ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ

3.1 Технологія Extended detection and response від Palo Alto Networks

У цьому розділі розглянемо можливості рішення XDR від Palo Alto Networks та як його можна використовувати у розрізі організації кіберстійкості. Як вже було згадано раніше, кіберстійкість включає в себе такі компоненти, як:

- захист кінцевих точок від:
    - шкідливих програм, так як: viruses, trojans, ransomware, spyware, crypto miners та ін.
    - шкідливих макросів, вбудованих у файли Microsoft Office
    - спроб викрадення облікових даних з пам’яті або мережевого трафіку
    - зловмисної поведінки запущених файлів, процесів, змін реєстру та/або доступу до пам’яті
    - розвідувальних атак (сканування)
    - спроб використання зловмисних веб-сторінок і використанню тактик, вбудованих у легітимні веб-сайти
    - несанкціонованих маніпуляцій з боку неавторизованих користувачів
    - бокових переміщень та ін.
- консолідація даних з різних джерел задля об’єднання сповіщень безпеки в інциденти;
- threat hunting – проактивний пошук загроз;
- моніторинг подій в реальному часі;
- оцінка знайдених вразливостей та їх класифікація;
- розслідування інцидентів;
- інвентаризація систем та додатків;
- виявлення застарілих версій систем і додатків та ін.

Усі ці можливості містить в собі рішення Extended detection and response від Palo Alto Networks (таблиця 3.1).

Таблиця 3.1

Можливості рішення EDR від Palo Alto Networks

№	Можливості	Опис можливості	
1	Системне адміністрування та огляд	1.1	Єдина консоль для перегляду подій та інцидентів з різних джерел (таких як NGFW, Data Lake, CotrexXDR тощо)
		1.2	Звіти, створені на вимогу, заплановані звіти та звіти електронною поштою
		1.3	Налаштування агенту, захист від зловмисного програмного забезпечення, експлойтів; обмеження та виключення
		1.4	Застосування профілів до різних систем та/або груп систем
		1.5	Можливість створення статичних, динамічних груп та груп активного каталогу
		1.6	Можливість створення правил BIOC
		1.7	Можливість створення правил IOC
		1.8	Створення Alert Exclusion Policy, щоб виключити відображення певних сповіщень на консолі
		1.9	Встановлення інсталяційних пакетів Windows, Linux, Mac
		1.10	Адміністрування агентів, що включає: оновлення та видалення агентів, сканування за вимогою, ізоляція хосту

Продовження табл. 3.2

№	Можливості	Опис можливості	
		1.11	Видимість сповіщень та сканування файлів
		1.12	Incident Management: включає групування попереджень, assignment, опис, критичність, розслідування інцидентів, примітки до інцидентів, статус
2	Виявлення та запобігання загрозам	2.1	Reconnaissance: надає можливість визначати та/або блокувати розвідувальні атаки (сканування)
		2.2	Credential Access: визначає та блокує спроби викрадення облікових даних з пам’яті (credential dump, brute force) або мережевого трафіку (ARP spoofing, DNS Responder)
		2.3	Malware Threat Protection: виявляє шкідливі програми (включаючи viruses, trojans, ransomware, spyware, crypto miners) та запобігає їх запуску
		2.4	Behavioral Threat Protection: виявляє та запобігає зловмисній поведінці запущених файлів, процесів, змін реєстру та/або доступу до пам’яті
		2.5	Office File Macro Protection: визначає та запобігає запуск шкідливих макросів, вбудованих у файли Microsoft Office
		2.6	Browser Exploit Protection: виявляє та запобігає спробам використання зловмисних веб-сторінок і використанню тактик, вбудованих у легітимні веб-сайти
		2.7	Defense Evasion Detection: внутрішній механізм захисту від доступу та маніпуляцій з боку неавторизованих користувачів
		2.8	Lateral Movement: ідентифікує та блокує / сповіщає про lateral movement (SMB relay, pass the hash)

Прожовження табл. 3.2

№	Можливості	Опис можливості	
		2.9	Anomalous Behavior Detection: визначає дії систем, користувачів і процесів, які відрізняються від їх нормальної поведінки, і ідентифікує потенційно скомпрометовані системи та облікові записи
		2.10	Deception Detection: виявляє взаємодії з приманками (decoys), які наявні в IT-інфраструктурі компанії
		2.11	Exfiltration Detection: визначає факт викрадення даних за допомогою легітимних протоколів (DNS tunneling, ICMP tunneling). Також визначає та блокує використання відомих інструментів для атак (Metasploit, Empire, Cobalt тощо)
3	Розслідування та моніторинг	3.1	System Activity Collection: Cortex XDR збирає та надсилає дані про виявлені спрацювання на робочих станціях та серверах
		3.2	Vulnerability Management: Cortex XDR проводить оцінку вразливостей файлів у системі
		3.3	Query Language Capabilities: Cortex XDR здійснює пошук серед необроблених і оброблених даних за допомогою query-запитів і представляє результати в зручному для користувача форматі (демонстрація Predifiened Templates from Query Library)
		3.4	Threat Hunting: Cortex XDR підтримує розслідування інцидентів за допомогою запитів для пошуку в рамках інциденту, виконання активних дії та кореляції даних
		3.5	Execute Forensic Investigation: демонстрація вбудованих інструментів для проведення розслідування спрацювань на робочих станціях та серверах

Продовження табл. 3.2

№	Можливості	Опис можливості	
		3.6	Demonstrate Host Inventory: Cortex XDR проведення інвентаризації додатків, встановлених на контрольованих системах
		3.7	Можливість кореляцій подій з різних джерел (NGFW, Data Lake, CotrexXDR agent) в єдиний інцидент
		3.8	Можливість побудови дерева причинно-наслідкового звязку в якому фігурують події з різних джерел
		3.9	XDR дозволяє проводити детальний пошук по подіям в NGFW за допомогою використання мови XQL
4	Контроль і відновлення	4.1	Search And Destroy: агент Cortex XDR створює локальну базу даних на кінцевій точці зі списком усіх файлів, включаючи їх шлях, хеш і додаткові метадані. Наявність функціоналу видалення всіх екземплярів небезпечного файлу на кінцевих точках безпосередньо з Cortex XDR
		4.2	Script Execution: можливість запуску скриптів на Python 3.7 на кінцевих точках з Cortex XDR. Демонстрація вбудованих сценаріїв для Cortex XDR (pre-canned scripts)
		4.3	EDL: External Dynamic List (EDL) — це текстовий файл, розміщений на зовнішньому веб-сервері, який використовує фаєрвол Palo Alto Networks для забезпечення контролю над доступами користувачів до IP-адрес і доменів, які Cortex XDR виявив в рамках інциденту
		4.4	Remediation Suggestions: рекомендації щодо усунення наслідків зловмисної діяльності

Продовження табл. 3.2

№	Можливості	Опис можливості	
		4.5	Remote Operations (Live Terminal): Live Terminal дозволяє керувати віддаленими кінцевими точками для розслідування та реагування, включаючи можливість навігації та керування файлами у файловій системі
		4.6	Host Firewall Cortex XDR: дозволяє контролювати мережеві з'єднання на кінцевих точках, не оновлюючи налаштування фаєрвола Windows або Mac
		4.7	Threat Hunting for IOC: демонстрація додавання правила IOC в рамках інциденту
		4.8	Device Control: контроль за підключенням до кінцевих точок змінних носіїв, дисководів, компакт-дисків та інших портативних пристроїв, які можуть містити шкідливі файли
		4.9	File Execution: контроль виконання файлів на кінцевих точках, використовуючи хеші файлів, включені у списки дозволів і блокувань
		4.10	Custom Threat Prevention: можливість створення користувацьких правил, що дозволяють налаштовувати та застосовувати визначені користувачем правила BIOC до профілів обмеження (Restrictions profiles)
5	Архітектура та додаткові компоненти	5.1	Resource Utilization: мінімальне навантаження на кінцеві точки/сервери агентом Cortex XDR в стані спокою
		5.2	Threat Intelligence: дозволяє розслідувати артефакти в рамках інциденту за допомогою запитів до таких систем, як: AutoFocus, VirusTotal, WildFire

Продовження табл. 3.2

№	Можливості	Опис можливості	
		5.3	Notification Forwarding: можливість пересилання сповіщень за допомогою конфігурацій (тип журналу), який потрібно пересилати
		5.4	Disk Encryption: Cortex XDR забезпечує повну видимість зашифрованих кінцевих точок Windows і Mac, які були зашифровані за допомогою BitLocker і FileVault відповідно
		5.5	Log Retention: Cortex XDR забезпечує збір і збереження журналів
		5.6	Single Sign-On (SSO) Scope Based Access Control: Cortex XDR підтримує підключення до Active Directory і SSO через SAML
		5.7	3rd Party Tools Compatibility: взаємодія з стандартним програмним забезпеченням на кінцевих точках або серверах
		5.8	Offline Prevention Support: Cortex XDR забезпечує повний захист кінцевих точок і серверів, які знаходяться в автономному режимі

Опис ключових компонентів рішення

Розгортання Cortex XDR, яке використовує повний набір сенсорів, може містити такі компоненти (табл. 3.2):

- Cortex XDR — додаток Cortex XDR забезпечує повну видимість усіх ваших даних на рівні даних Cortex. Програма надає єдиний інтерфейс, за допомогою якого ви можете досліджувати та сортувати сповіщення, вживати заходів щодо виправлення та визначати політики для виявлення зловмисної діяльності в майбутньому.

- Cortex Data Layer — рівень даних у Cortex XDR tenant, який зберігає журнали всіх типів даних.
- Cortex XDR Pro per TB:
    - Analytics engine — це служба безпеки, яка використовує мережеві дані для автоматичного виявлення загроз після вторгнення та звітування про них. Механізм аналітики робить це шляхом виявлення належної (нормальної) поведінки у вашій мережі, щоб він міг помітити погану (аномальну) поведінку.
    - Palo Alto Networks next-generation firewalls — локальні або віртуальні фаєрволи, які забезпечують дотримання політик безпеки мережі у ваших офісах, філіях і хмарних центрах обробки даних.
    - Palo Alto Networks Prisma Access and GlobalProtect — якщо ви поширите свою політику безпеки фаєрвола на мобільних користувачів і віддалені мережі за допомогою Prisma Access або GlobalProtect, ви також зможете пересилати відповідні журнали трафіку, включно з журналами IoT, до Cortex Data Lake. Потім аналітичний механізм може аналізувати ці журнали та подавати сповіщення про аномальну поведінку.
    - External firewalls and alerts — Cortex XDR може отримувати журнали трафіку від зовнішніх постачальників фаєрволів, наприклад Check Point, і використовувати аналітичну систему для аналізу цих журналів і попередження про аномальну поведінку. Щоб отримати додатковий контекст у ваших інцидентах, ви також можете надсилати сповіщення із зовнішніх джерел сповіщень.
- Cortex XDR Pro per Endpoint:
    - Analytics engine — аналітика Cortex XDR також може використовувати дані кінцевих точок для автоматичного виявлення загроз після вторгнення та звітування про них. Механізм аналітики може використовувати дані кінцевої точки, щоб надсилати

сповіщення про ненормальну поведінку мережі (наприклад, сканування портів).

o Cortex XDR agents — захищає кінцеві точки від відомих і невідомих шкідливих програм, зловмисної поведінки та методів. Агенти Cortex XDR виконують власний аналіз локально на кінцевій точці, але також використовують інформацію про загрози WildFire. Агент Cortex XDR повідомляє про всю діяльність кінцевої точки на рівень даних Cortex для аналізу програмами Cortex XDR.

o External alert sources — щоб додати до ваших інцидентів додатковий контекст, ви можете надсилати сповіщення Cortex XDR із зовнішніх джерел за допомогою Cortex XDR API.

Таблиця 3.2

Критерії оцінки рішення

№	Критерії оцінки	Опис
1	Єдина консоль для перегляду подій та інцидентів з різних джерел (XDR agent, NGFW, Data Lake тощо) та глибинний пошук по подіям в NGFW	Даний функціонал зменшує час на аналітику подій та дає розуміння, що було причиною інциденту на NGFW та чи була дана активність заблокована
2	Додавання користувачів до консолі управління, налаштування ролей та привілеїв	Тестування можливості створення користувачів та адміністраторів, змінення їх ролей, прав та привілеїв
3	Генерація агента та інсталяція на кінцеві точки	Можливість генерації агентів у консолі рішення, їх вивантаження та інсталяції на кінцевих точках
4	Підтримка режиму Alert агента	Підтримка агентів режиму Alert, в якому до загроз застосовуються лише сповіщення

Продовження табл. 3.2

№	Критерії оцінки	Опис
5	Підтримка режиму Prevent агента	Підтримка агентів режиму Alert, в якому до загроз застосовуються як сповіщення, так і блокування
6	Запобігання (блокування) атакам та зловмисному програмному забезпеченню	Блокування роздвідувальних атак, шкідливого програмного забезпечення, виявлення зловмисної поведінки файлів, блокування шкідливих макросів та ін.
7	Відображення сповіщень в інтерфейсі консолі та наявність нотифікацій нотифікації	Наявність графічних консолей та їх оновлення у режимі реального часу, можливість надсилати сповіщення про події на пошту та за допомогою syslog
8	Формування схем та відображення поетапного процесу атаки	Відображення інцидентів що демонструють зв’язки, статистику та покроковий аналіз подій
9	Підтримка ізоляції хостів	Тестування можливості ізоляції хостів у випадку їх зараження
10	Використання LiveTerminal з центральної консолі на кінцевій точці	Можливість з консолі управління за допомогою LiveTerminal виконувати команди на кінцевих точках
11	Скасування застосованих змін на кінцевих точках	Наявність функціоналу відновлення та скасування запроваджених змін на тестових робочих станціях замовника

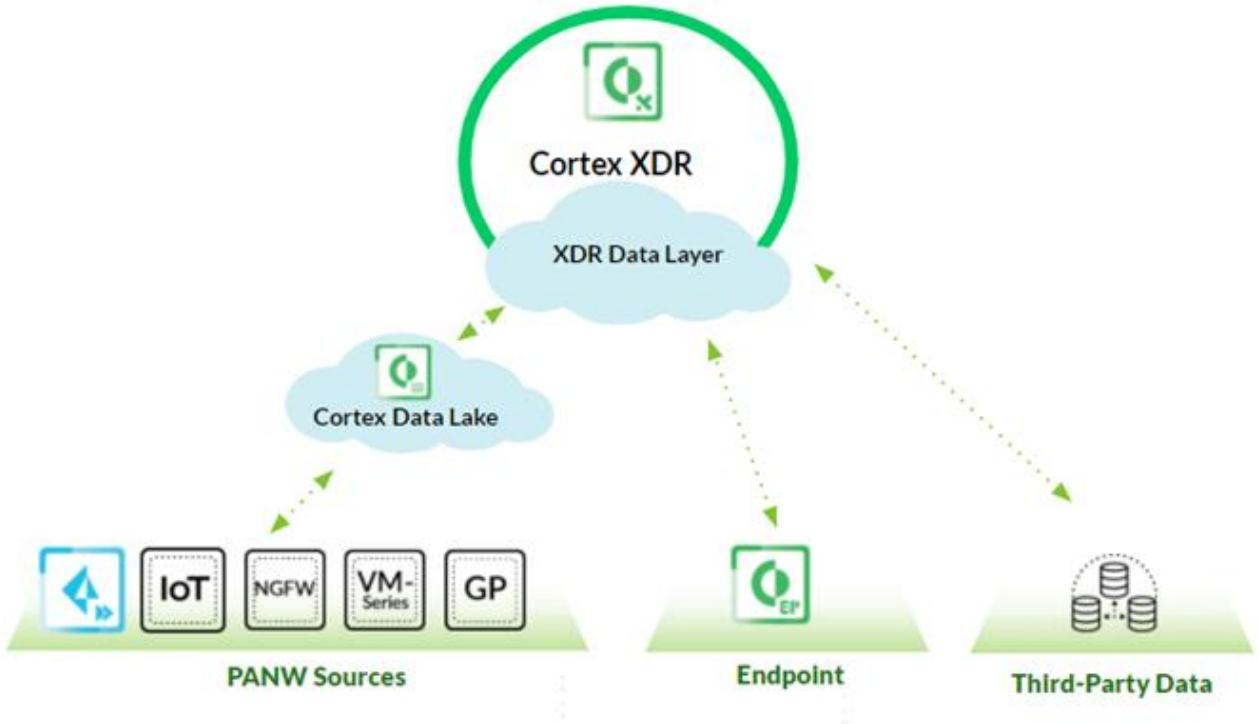

Рис. 3.1 Архітектурна схема рішення

3.2 Технологія Cortex XDR, як один із інструментів забезпечення кіберстійкості

Захист кінцевих точок

Кібератаки націлені на кінцеві точки, щоб завдати шкоди, викрасти інформацію або досягти інших цілей, які включають контроль над комп'ютерними системами. Зловмисники здійснюють кібератаки, змушуючи користувача ненавмисно запустити зловмисний виконуваний файл або використовуючи слабкість у законному виконуваному файлі для запуску зловмисного коду у фоновому режимі без відома користувача [17].

Один із способів запобігти цим атакам — визначити виконувані файли, бібліотеки динамічного компонування (DLL) та інші фрагменти коду, щоб визначити, чи є вони зловмисними, і, якщо так, запобігти виконанню цих компонентів, спочатку зіставивши кожен потенційно небезпечний код зі списком конкретних відомих сигнатур загроз. Слабкість цього методу полягає в тому, що антивірусні рішення на основі сигнатур (AV) займають багато часу для виявлення новостворених загроз, які відомі лише зловмиснику (також відомі як

атаки нульового дня або експлойти), і додавання їх до списків відомих загроз, що робить кінцеві точки вразливими, доки сигнатури не оновляться.

Cortex XDR використовує ефективніший і дієвіший підхід до запобігання атакам, який усуває потребу в традиційній антивірусній системі. Замість того, щоб намагатися йти в ногу зі списком відомих загроз, що постійно зростає, Cortex XDR встановлює низку блокпостів, які також називають пастками, які запобігають атакам у початкових точках входу — точці, де законні виконувані файли збираються потрапити несвідомо допускати зловмисний доступ до системи.

Cortex XDR надає багатометодне рішення захисту з модулями захисту від експлойтів, які спрямовані на уразливості програмного забезпечення в процесах, які відкривають невиконувані файли, і модулями захисту від зловмисного програмного забезпечення, які перевіряють виконувані файли, бібліотеки DLL і макроси на наявність зловмисних підписів і поведінки. Використовуючи цей багатометодний підхід, Cortex XDR може запобігти всім типам атак, незалежно від того, чи є вони відомими чи невідомими [17].

Об’єднання сповіщень безпеки в інциденти

Атака може вплинути на кілька хостів або користувачів і викликати різні типи сповіщень, що випливають з однієї події. Усі артефакти, активи та сповіщення про загрозу збираються в Інцидент.

Логіка, за якою додаток Cortex XDR призначає інциденту, базується на наборі правил, які враховують різні атрибути. Приклади атрибутів сповіщення включають джерело сповіщення, тип і період часу. Програма витягує набір артефактів, пов’язаних із подією загрози, перелічених у кожному сповіщенні, і порівнює його з артефактами, які з’являються в існуючих сповіщеннях у системі. Сповіщення в одному ланцюжку причинно-наслідкових зв’язків групуються з одним інцидентом, якщо відкритий інцидент уже існує. В іншому випадку нове вхідне сповіщення створить новий інцидент.

Об’єднання сповіщень безпеки в інциденти допомогає фахівцям ІБ бачити більш повну картину та оперативно реагувати (рис. 3.2). Автоматизація є

необхідною складовою в питанні побудови стратегії кіберзахисту організації, так як без неї неможливо ефективно побудувати захист через те, що уйма часу буде витрачено на рутинну роботу, яка виснажує фахівців інформаційної безпеки. Сортування, об'єднання алертів в інциденти та оцінка ризику кожного сповіщення безпеки. допомагає вчасно та реагувати на події безпеки враховуючи їх критичність.

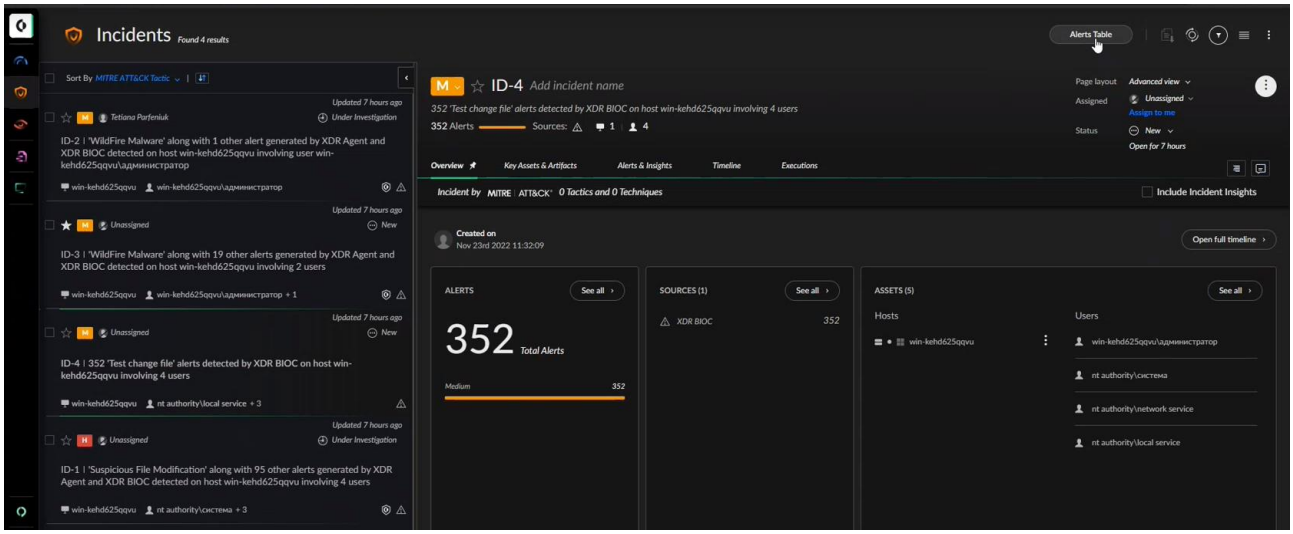

Рис 3.2 Об’єднання сповіщень безпеки в інциденти

Моніторинг подій в реальному часі

Сторінка «Інциденти» відображає всі інциденти в консолі керування Cortex XDR, щоб допомогти вам визначити пріоритети, відстежувати, сортувати, досліджувати та вживати заходів для виправлення (рис 3.2) [18].

Також рішення має предналаштовані панелі, які допомагають фахівцям консолідовано розглядати події безпеки в інфраструктурі. Рішення пропонує наступні предналаштовані панелі:

- Agent Management Dashboard (рис. 3.3)

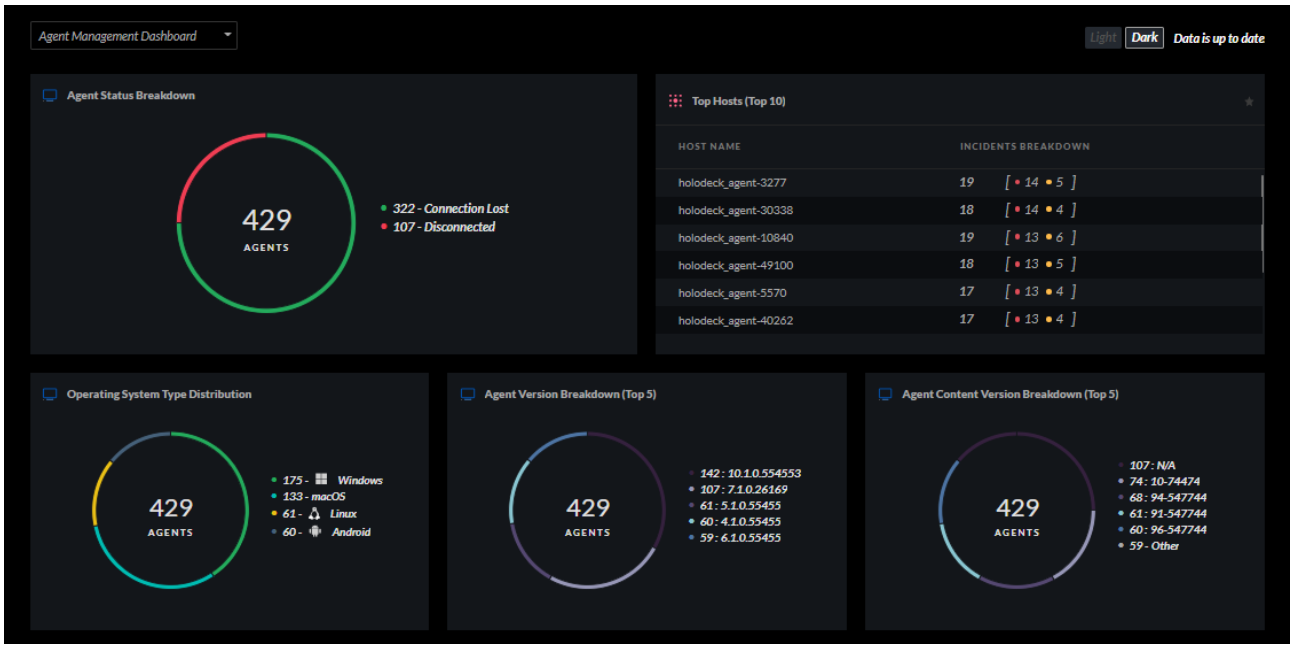

Рис. 3.3 Панель Agent Management Dashboard

- Cloud Inventory Dashboard (рис. 3.4)

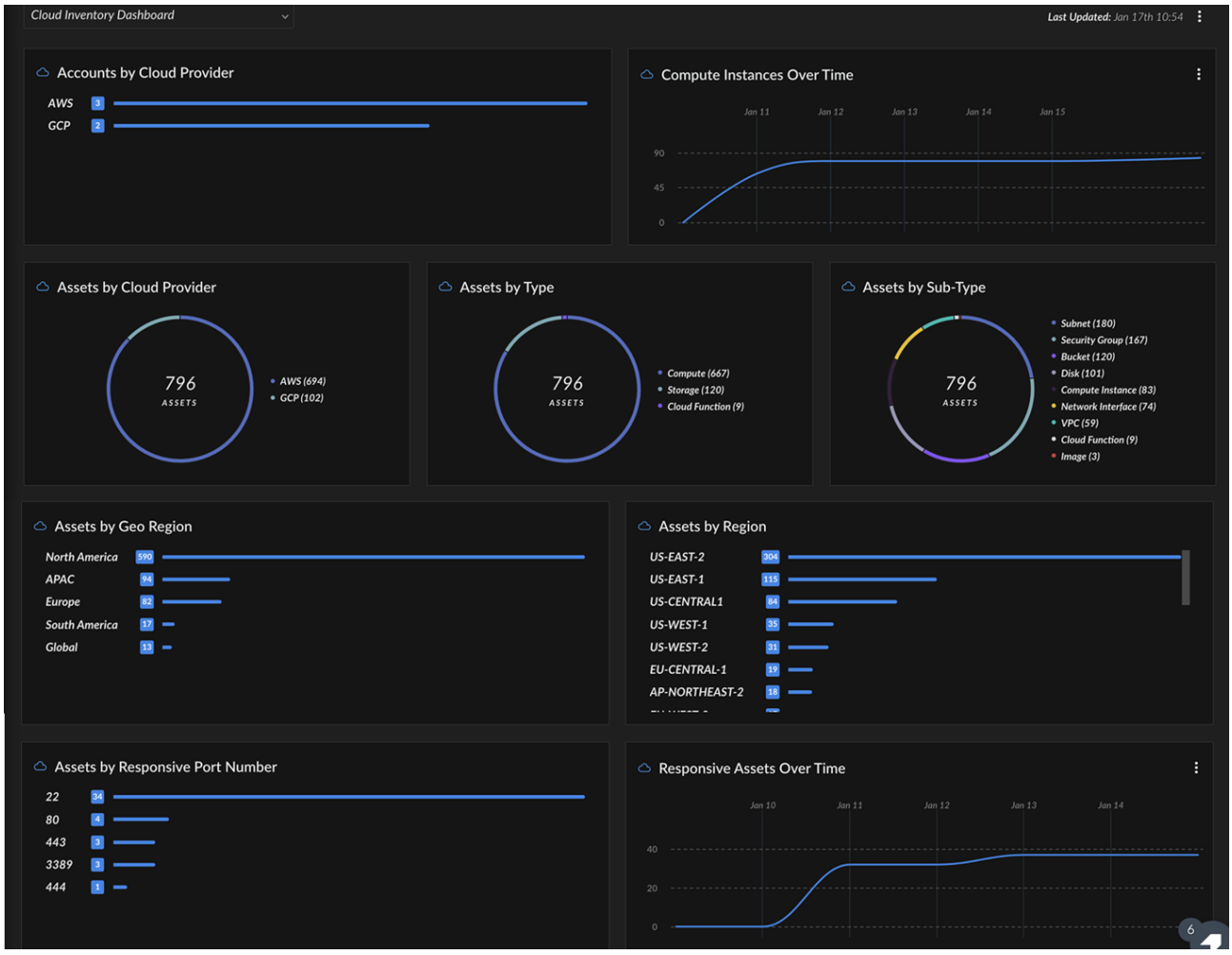

Рис. 3.4 Панель Cloud Inventory Dashboard

- Data Ingestion Dashboard (рис. 3.5)

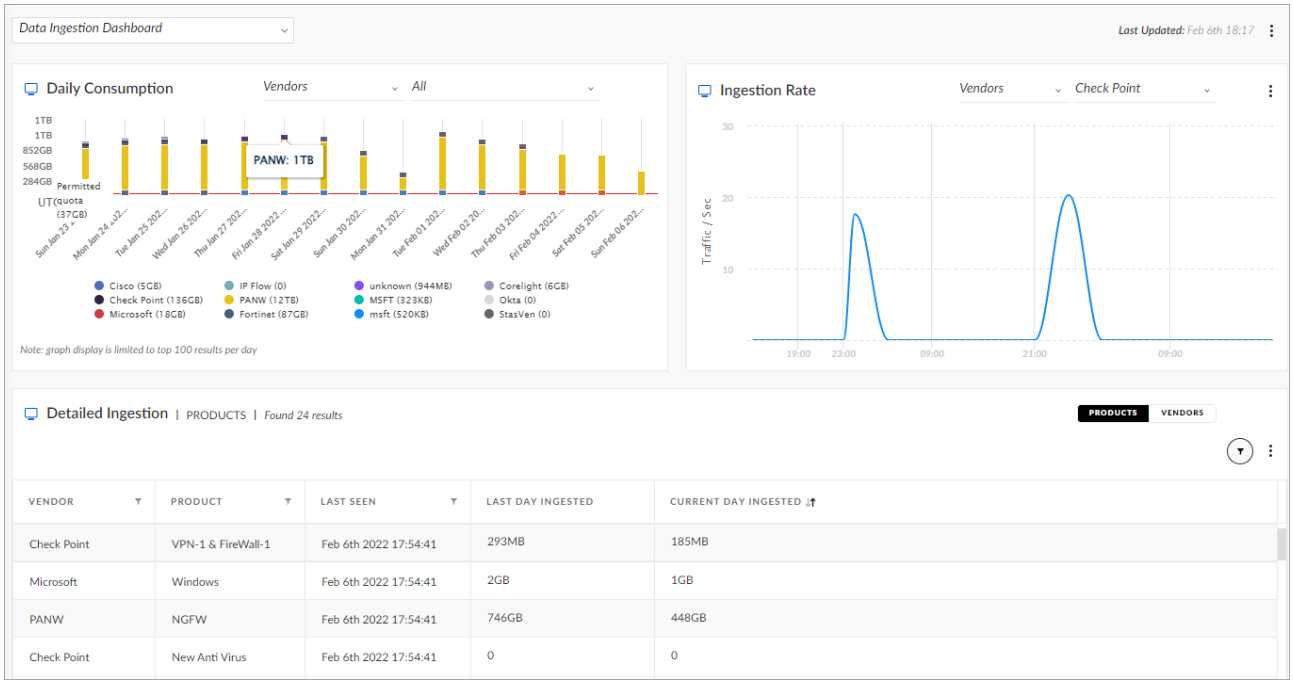

Рис. 3.5 Data Ingestion Dashboard

- Incident Management Dashboard (рис. 3.6)

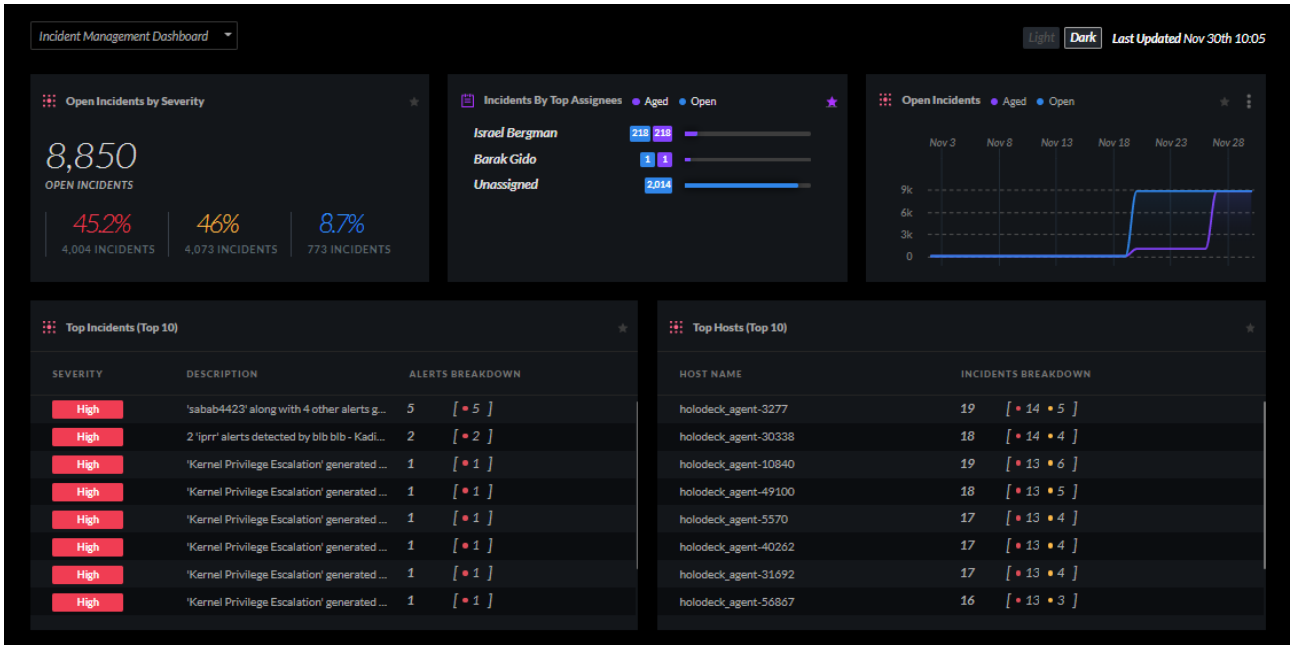

Рис. 3.6 Панель Incident Management Dashboard

- Network Traffic Analysis (NTA) Dashboard

Інформаційна панель аналізу мережевого трафіку (NTA) допомагає краще візуалізувати та відстежувати мережевий трафік Cortex XDR [18].

Інформаційна панель складається з таких віджетів:

➢ Overview – огляд;

- ➢ Threats – загрози;
- ➢ Network Zones – зони мережі;
- ➢ Geo Locations – геолокації;
- ➢ DNS Activity – DNS-активність;
- ➢ HTTP Activity – активність HTTP;
- ➢ URL Activity – URL-активність [18].

- My Dashboard (рис. 3.7)

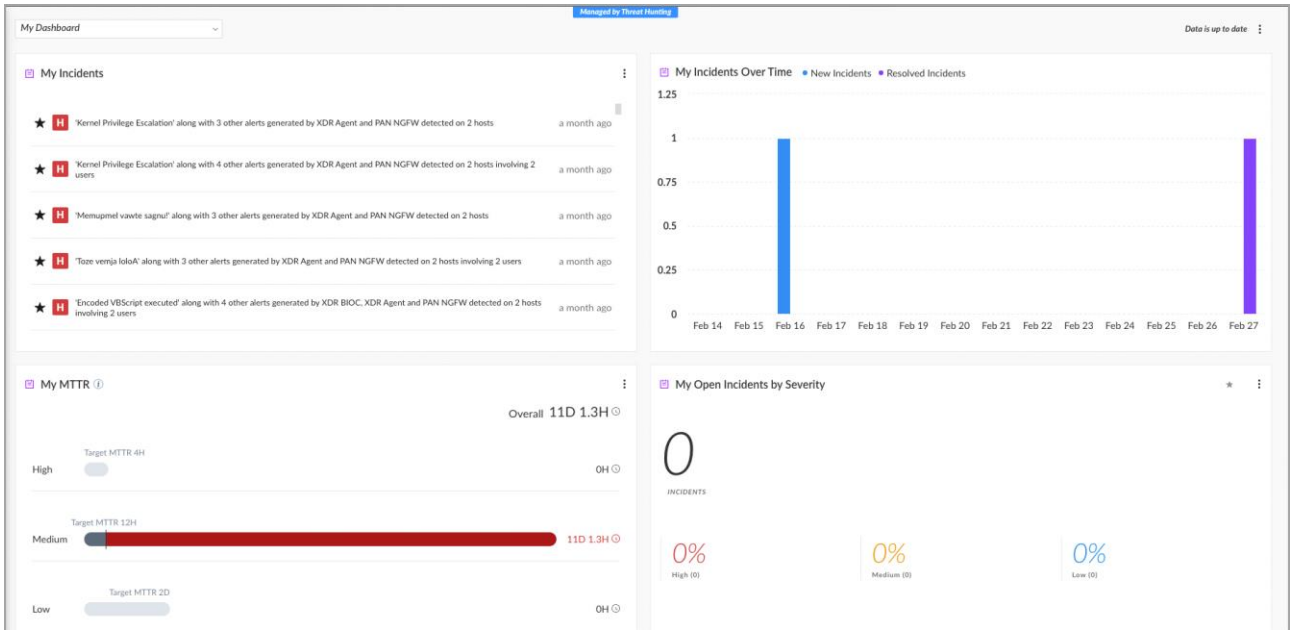

Рис. 3.7 Панель My Dashboard

- Security Admin Dashboard (3.8)

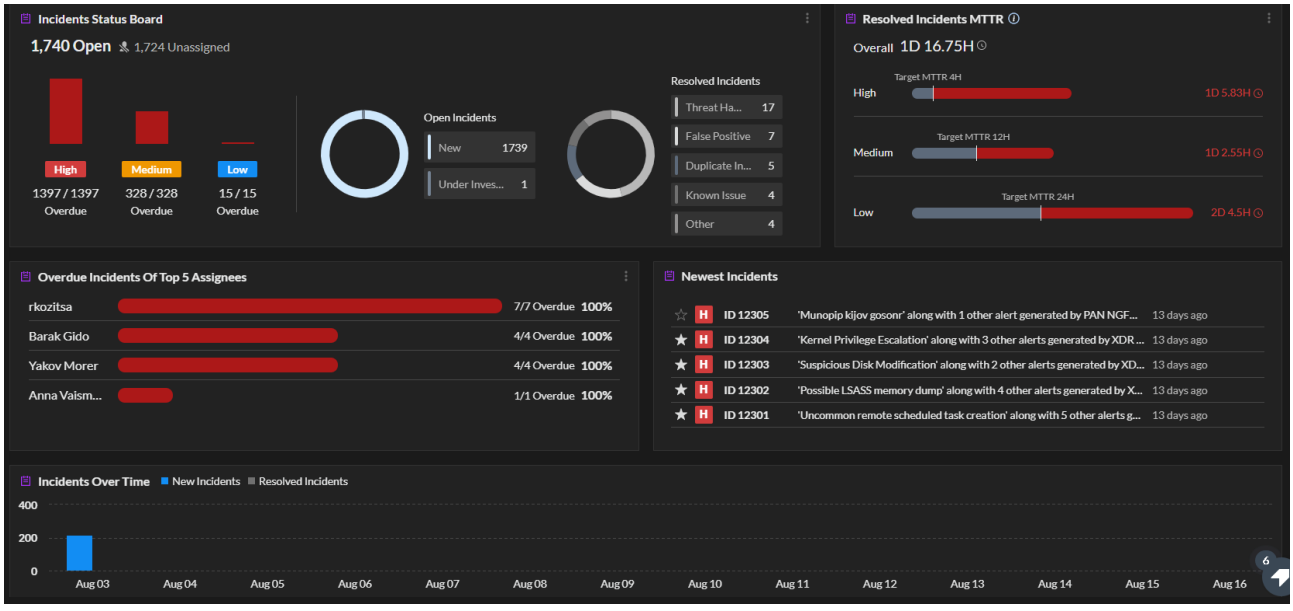

Рис. 3.8 Панель Security Admin Dashboard

- Security Manager Dashboard (рис. 3.9)

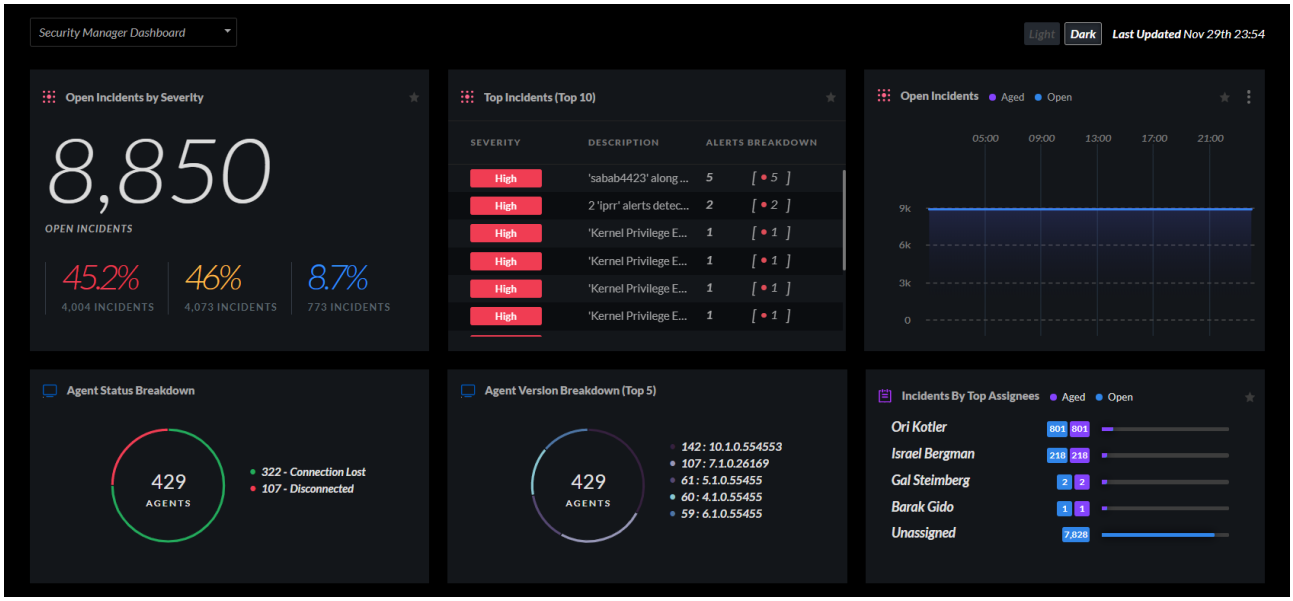

Рис. 3.9 Security Manager Dashboard

У разі, коли жоден з шаблонів повністю не задовольняє потребам є можливість або модифікувати будь який з шаблонів і додати необхідні предналаштовані віджети, або з нуля створити та зберегти саме таку панель, щоб вона повність відповідала потребам компанії (рис. 3.10).

Дане рішення є досить гнучким в налаштуванні, тому надає можливість самостійно створити специфічні віджети за допомогою XQL Query, якщо серед вбудованих не знайшлось необхідного.

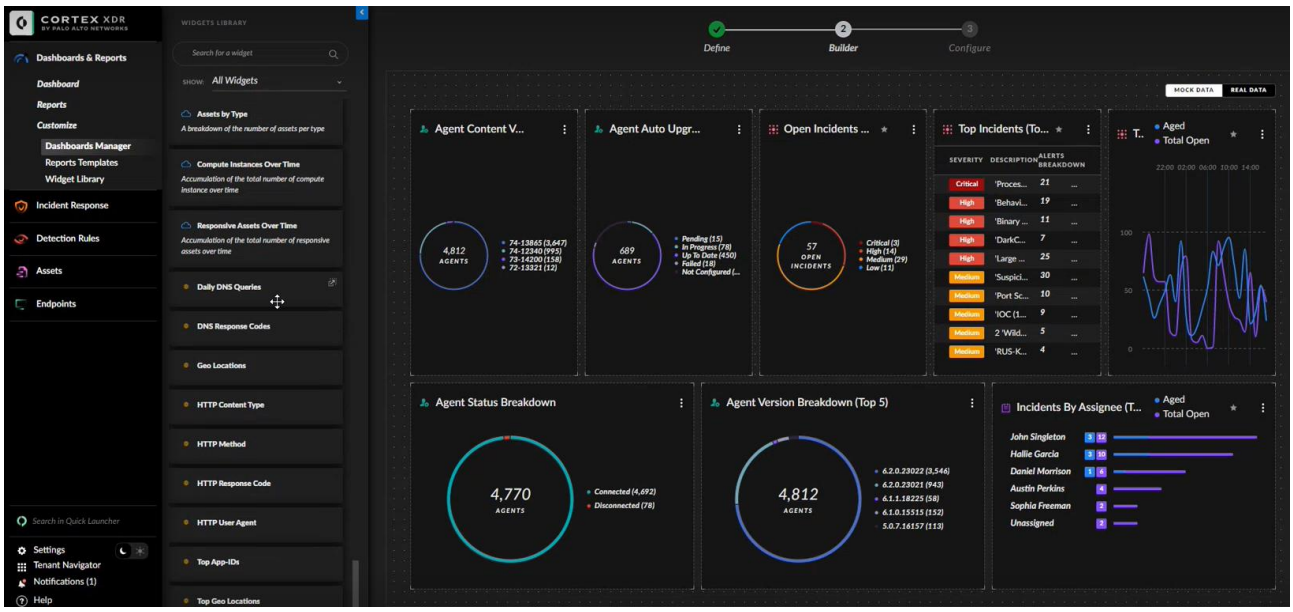

Рис. 3.10 Менеджер для створення власних панелей

Threat hunting – проактивний пошук загроз. Оцінка знайдених вразливостей та їх класифікація

Вкладка «Огляд» відображає тактику та методи MITER (рис 3.12), підсумкову шкалу часу та інтерактивні віджети, які візуалізують кількість сповіщень, типи джерел, хостів і користувачів, пов’язаних з інцидентом (рис. 3.11) [19]

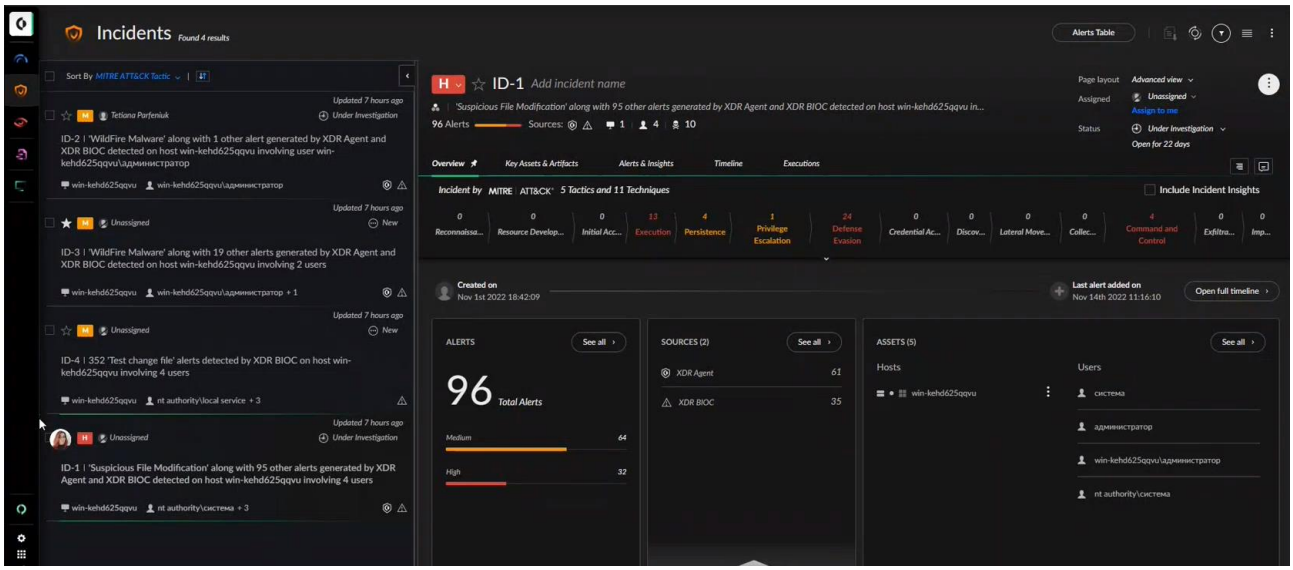

Рис. 3.11 Вкладка «Огляд»

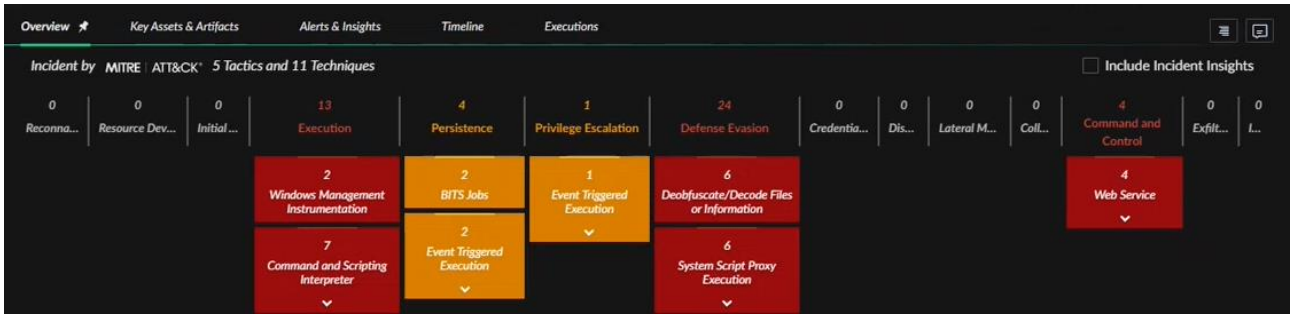

Рис. 3.12 Тактики та методи MITER, які містить в собі інцидент

Вкладка «Ключові активи та артефакти» відображає всю інформацію про інциденти та артефакти хостів, користувачів і ключові артефакти, пов’язані з інцидентом (рис. 3.13). У розділі «Артефакти» ви можете знайти і переглянути артефакти, пов’язані з інцидентом [19]. Кожен артефакт відображає, якщо доступно, інформацію про артефакт і доступні дії відповідно до типу артефакту: файл, IP-адреса та домен.

У розділі «Хости» знайдіть і перегляньте хости, пов’язані з інцидентом. Кожен хост відображає, якщо доступно, таку інформацію про хост і доступні дії:

- Відомості про власника;
- Дії хоста [19]

Щоб детальніше дослідити хост:

Виберіть ім’я хоста, щоб відобразити панель подробиць. Панель доступна лише для хостів із інстальованим агентом і відображає ім’я хоста, незалежно від того, чи він під’єднаний, а також відомості про кінцеву точку, відомості про агента, мережу та інформацію про політику. Крім того, ви можете виконувати доступні дії, перелічені у верхньому правому куті (рис. 3.13).

У розділі «Користувачі» знайдіть і перегляньте користувачів, пов’язаних з інцидентом. Кожен користувач відображає, якщо доступна, така інформація користувача та доступні дії:

- Відомості про користувача
- Дії користувача [19]

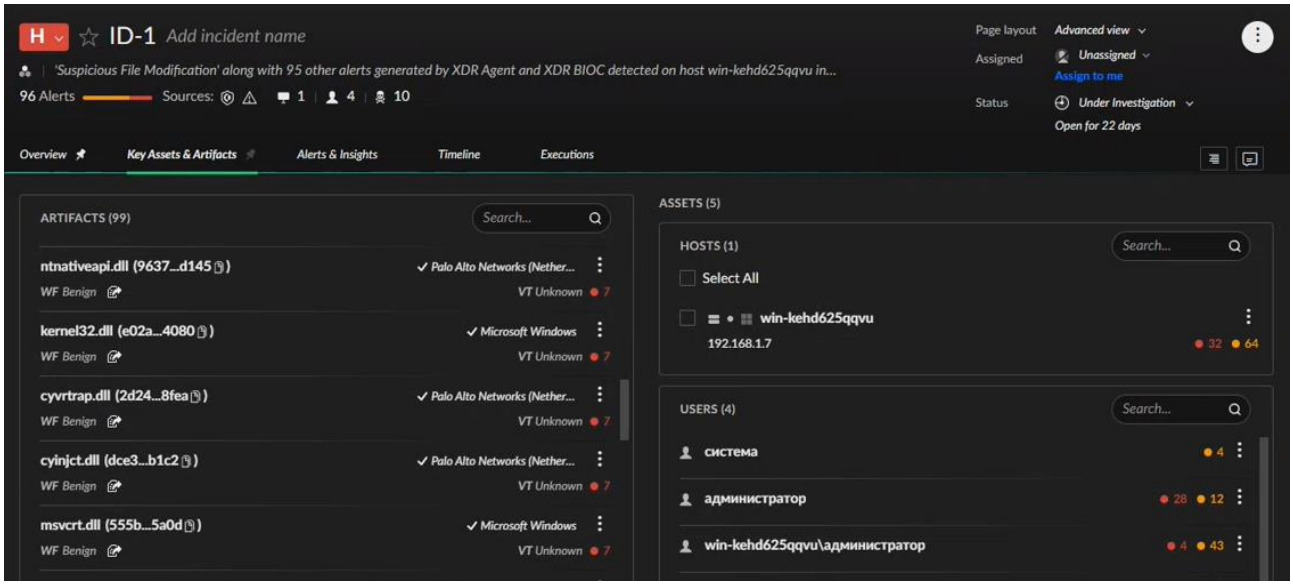

Рис. 3.13 Вкладка «Ключові активи та артефакти»

На вкладці Alerts & Insights відображається таблиця сповіщень і статистичних даних, пов’язаних з інцидентом (рис. 3.14) [19].

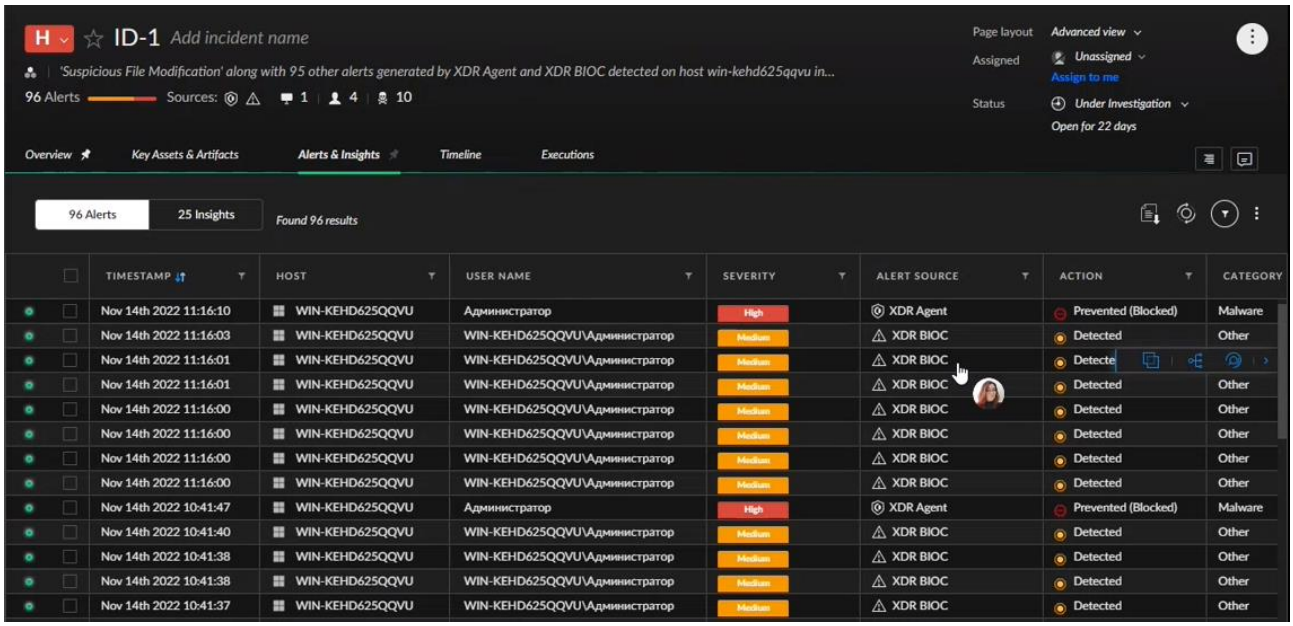

Рис. 3.14 Вкладка Alerts & Insights

Вкладка «Шкала інциденту» — це хронологічне представлення сповіщень і дій, пов’язаних з інцидентом (рис. 3.15). Кожен запис часової шкали є представленням типу дії, яка була ініційована в сповіщенні. Сповіщення, які містять однакові артефакти, групуються в один запис на часовій шкалі та відображають загальний артефакт в інтерактивному посиланні [19]. Залежно від типу дії ви можете вибрати запис, імена хостів і артефакти для подальшого дослідження дії.

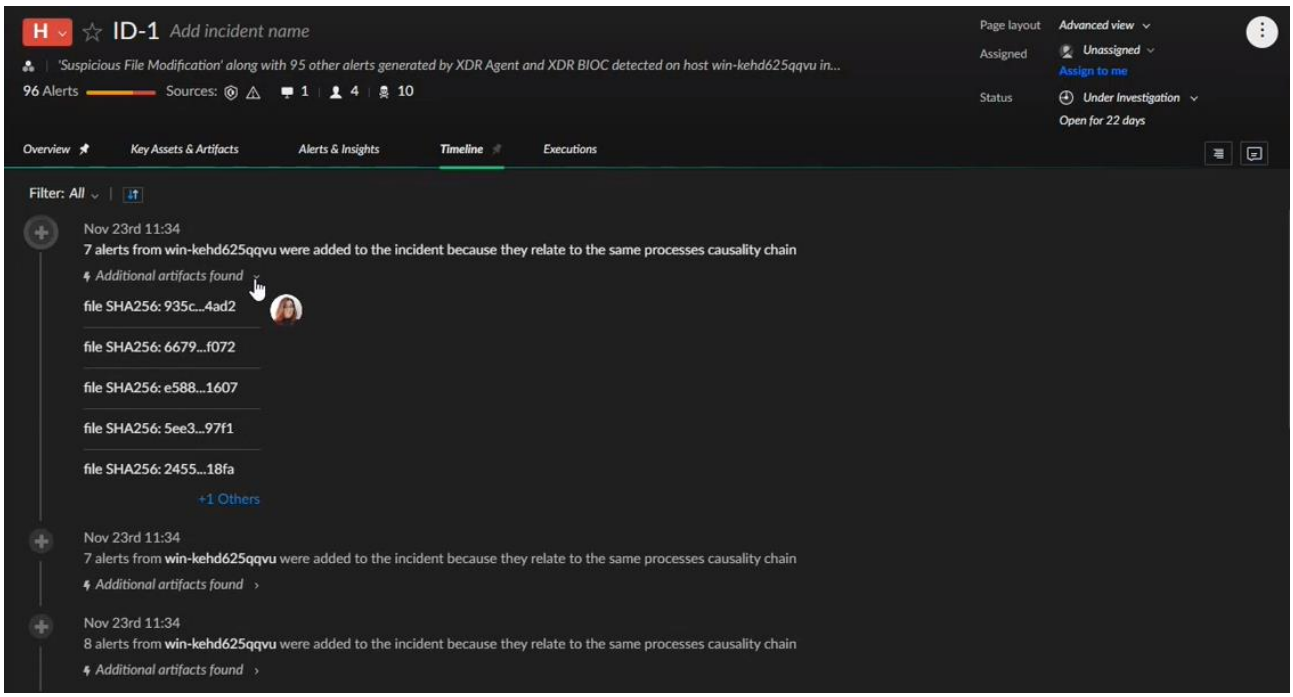

Рис. 3.15 Вкладка «Шкала інциденту»

На вкладці «Виконання» відображаються всі ланцюжки причинно-наслідкових зв’язків сповіщень, пов’язані з інцидентом (рис. 3.16). ааанцюги причинно-наслідкових зв’язків перераховані відповідно до власника групи причинності (Causality Group Owner – CGO), розгорніть картку CGO, яку ви хочете дослідити (рис. 3.17). На кожній картці CGO відображається ім’я CGO, такі деталі події CGO та ланцюжок причинності:

- Назва CGO;
- Джерела сповіщень, пов’язані з усім ланцюгом причинності;
- Час виконання ланцюжка причинності;
- Кількість сповіщень, які включають CGO відповідно до серйозності [19].

Для подальшого дослідження та виконання доступних дій перегляду причинності слід розкрити ланцюжок причинно-наслідкових зв’язків (рис. 3.18).

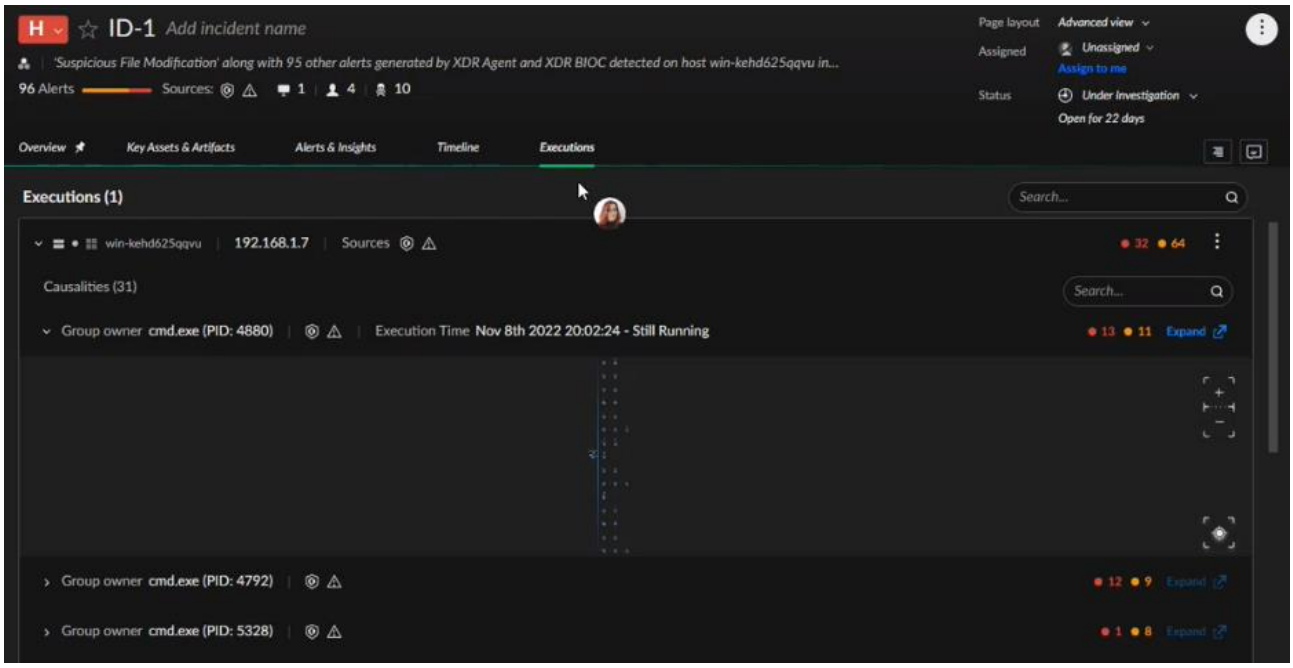

Рис. 3.16 Вкладка «Виконання»

Рис. 3.17 Ланцюг причинно-наслідкових зв’язків

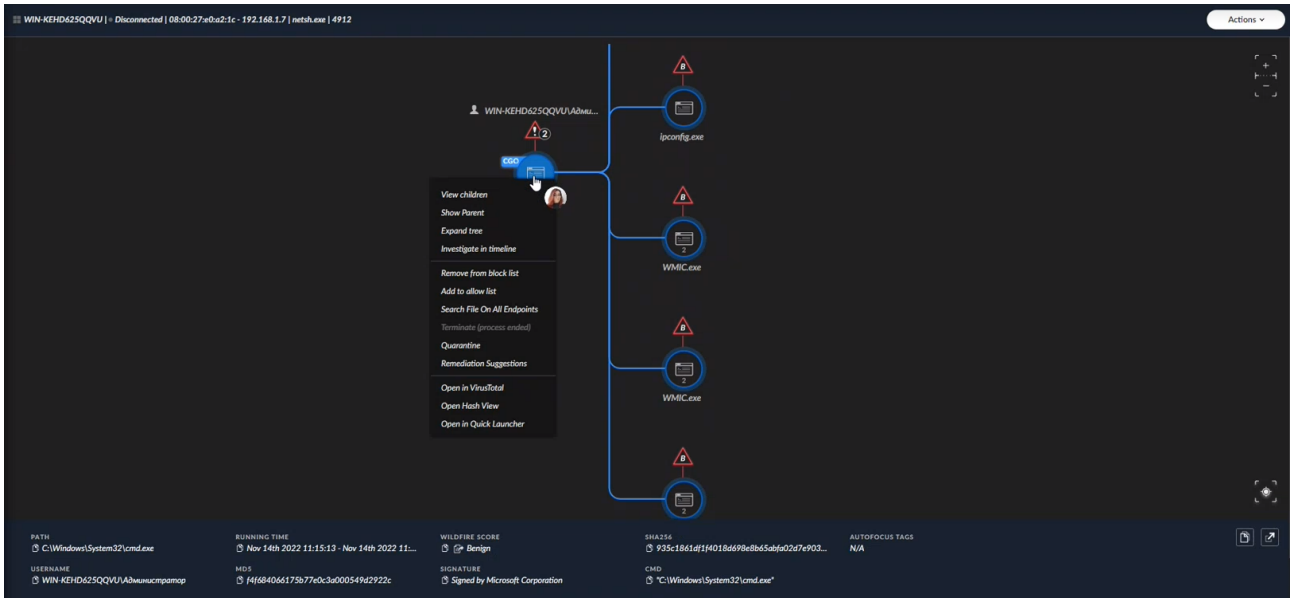

Рис. 3.18 Наявні дії для подальшого розслідування інциденту

Query Builder — це інструмент пошуку в основі Cortex XDR, який можна використовувати для швидкого пошуку та дослідження будь-якої інформації, виявлення першопричини попередження, проведення оцінки збитку та пошуку загроз із джерел даних, які комунікують з Cortex XDR (рис. 3.19) [20]. За допомогою Query Builder ви можете створювати складні запити для сутностей і атрибутів сутностей, щоб ви могли виявляти та ідентифікувати зв’язки між ними. Query Builder здійснює пошук у необроблених даних і журналах, і для вказаних вами сутностей і атрибутів повертає до 10 000 результатів [20].

У Query Builder ви також можете використовувати пошук XQL для створення запитів XQL для пошуку та перегляду необроблених даних, які

зберігаються в Cortex XDR або імпортуються з настроюваних і сторонніх наборів даних (рис 3.20) [20]

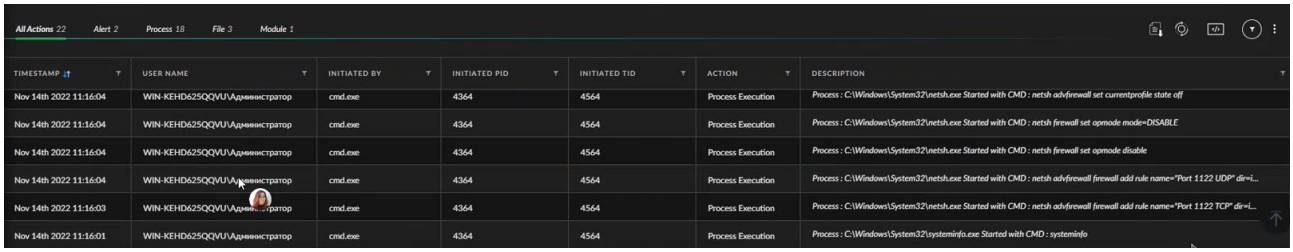

Рис. 3.19 Інструмент пошуку Query Builder

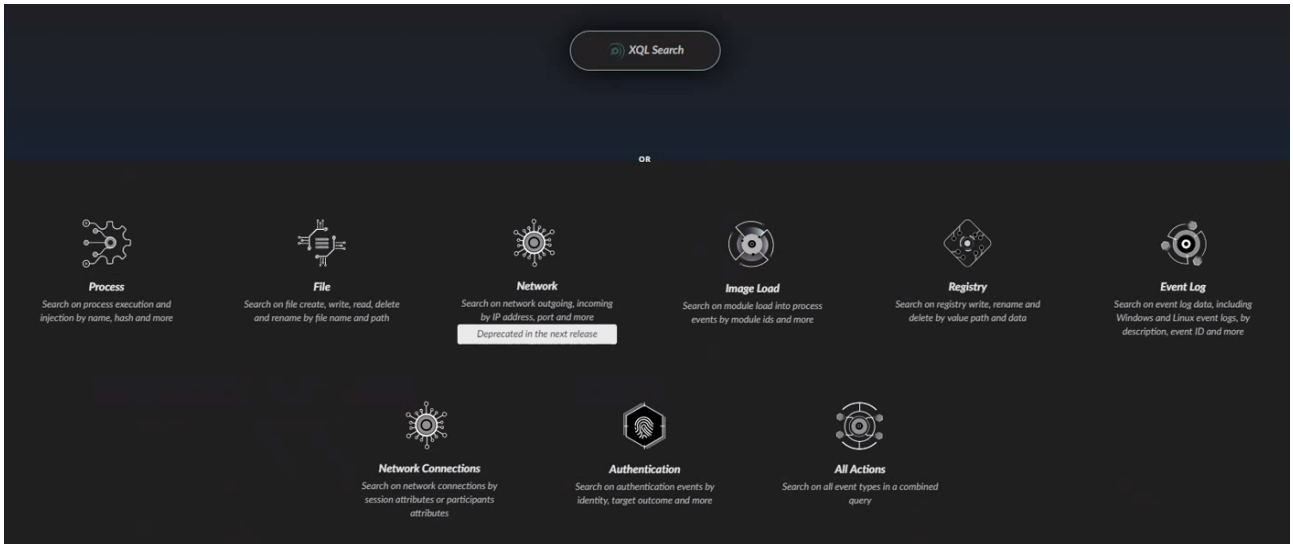

Рис. 3.20 Можливості використання пошуку XQL

Висновок до розділу 3

У даному розділі проаналізовано можливості технології XDR від Palo Alto Networks. Дана технологія була розглянута в контексті побудови та забезпечення кіберстійкості. За допомогою даного рішення можна закрити наступні питання безпеки: захист кінцевих точок, моніторинг подій в реальному часі, консолідація даних з різних джерел задля об’єднання сповіщень безпеки в інциденти, threat hunting, оцінка знайдених вразливостей та їх класифікація, розслідування інцидентів.

Слід зазначити, що дане рішення підходить компаніям (організаціям) лише у разі їх певної зрілості у питаннях кібербезпеки та достатньої кількості фахівців безпеки і бюджету.

ВИСНОВКИ

В роботі було досліджено поняття стійкості, бізнес стійкості та кіберстійкості. Розглянуто передумови виникнення концепції кіберстійкості. Використовуючи методи порівняння, узагальнення, синтезу та методи системного аналізу порівняно та зіставлено поняття кібербезпеки та кіберстійкості; проведено аналіз, досліджено особливості методів формування кібестійкості, як компонет стійкості бізнесу. Проаналізовано ключові компоненти, які повинен містити в собі план кіберстійкості. Запропонована методика впровадження плану з кіберстійкості.

В останньому розділі проаналізовано можливості технології XDR від Palo Alto Networks. Дана технологія була розглянута в контексті побудови та забезпечення кіберстійкості. За допомогою даного рішення можна закрити наступні питання безпеки: захист кінцевих точок, моніторинг подій в реальному часі, консолідація даних з різних джерел задля об’єднання сповіщень безпеки в інциденти, threat hunting, оцінка знайдених вразливостей та їх класифікація, розслідування інцидентів.

В роботі дійшли висновку, що кіберстійкість може бути реалізована лише за умови співпраці всіх зацікавлених сторін у бізнесі. Найкращий спосіб позбутися організаційних розривів і пояснити бізнесу, що кіберризики є відповідальністю кожного, це надати кожному можливість брати участь в управлінні ризиками. Від IT до інженерів, від C-suite до всіх співробітників, від партнерів бізнесу до сторонніх постачальників – кожен має усвідомити, що безпека – це питання бізнесу, а не лише технологічна проблема. Усі організаційні підрозділи мають бути обізнаними та виконувати свою роль у забезпеченні загальної кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Словник української мови, Академічний тлумачний словник (1970—1980) http://sum.in.ua/s/stijkyj

2. Kirvan P. O. What is business resilience?, 2022 https://www.techtarget.com/searchcio/definition/business-resilience

3. Brunskill V. L., Business continuity plan (BCP), 2022 https://www.techtarget.com/searchdisasterrecovery/definition/business-continuity-action-plan

4. Кіберстійкість – що це, як забезпечити та як управляти, 10Guards, 2018 URL: https://spilno.org/article/kiberstiikist-scho-tse-yak-zabezpechyty-ta-yak-upravlyaty

5. What is cyber resilience and how to improve it. URL: https://www.balbix.com/insights/what-is-cyber-resilience/

6. Linkov I. A., Kott A. L. Cyber Resilience of Systems and Networks. 2018/ URL: https://arxiv.org/ftp/arxiv/papers/1806/1806.02852.pdf

7. ISO 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary

8. ISO/IEC 27032 URL: https://pecb.com/en/education-and-certification-for-individuals/iso-iec-27032

9. Information Technology Laboratory, Computer Security Resource Center https://csrc.nist.gov/glossary/term/cyberspace

10. Cyber resilience and cybersecurity: what is the difference? URL: https://www.eurotechconseil.com/en/blog/difference-between-cyber-security-and-cyber-resilience/#:~:text=Experts%20on%20the%20subject%20will,and%20how%20it%20will%20recover

11. Ханна Д. О. Кібербезпека проти Кіберстійкість: чим вони відрізняються?, 2022 URL: https://spilno.org/article/kiberstiikist-scho-tse-yak-zabezpechyty-ta-yak-upravlyaty

12. CISO guide: 5 Steps to Improve Enterprise Cyber-Resilience, 2020. URL: https://www.balbix.com/app/uploads/CISO-Guide-5-Steps-to-Improve-Cyber-Resilience.pdf

13. Crocetti P. F. Emergency communications plan (EC plan) URL: https://www.techtarget.com/searchdisasterrecovery/definition/emergency-communications-plan-EC-plan

14. Cole B. D. What is a risk assessment? 2021. URL: https://www.techtarget.com/searchsecurity/definition/risk-assessment

15. Ross R. N., Pillitteri V. A., Graubart R. D. Developing Cyber-Resilient Systems NIST Special Publication 800-160. 2021. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf

16. Wallen D. N. Cyber Resilience and Its Importance for Your Business. 2022. URL: https://spanning.com/blog/cyber-resilience/

17. Endpoint Security Concepts. Cortex XDR Pro Administrator Guide. URL: https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Pro-Administrator-Guide/Endpoint-Security

18. Monitoring. Cortex XDR Pro Administrator Guide. URL: https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Pro-Administrator-Guide/Manage-Your-Cloud-Inventory-Assets

19. Manage Incidents. Cortex XDR Pro Administrator Guide. URL: https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Pro-Administrator-Guide/Triage-Incidents

20. Search Queries. Cortex XDR Pro Administrator Guide. URL: https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Pro-Administrator-Guide/The-Query-Builder