ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Рекомендації щодо виявлення та реагування на інциденти безпеки в кінцевих точках організації за допомогою TheHive 5»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

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

_____Олександр ЖУРАВЕЛЬ
(підпис)

Виконав: здобувач вищої освіти групи БСД-41
ЖУРАВЕЛЬ Олександр
(прізвище, ім'я)

Керівник к.військ.н., доцент ГАХОВ Сергій
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

ВСТУП

Актуальність дослідження. Виявлення та своєчасне реагування на інциденти безпеки в кінцевих точках організації має критичне значення з кількох причин. По-перше, кінцеві точки – це пристрої, такі як комп'ютери, ноутбуки та мобільні телефони, які взаємодіють з корпоративною мережею та обробляють конфіденційні дані. Компрометація цих пристроїв може призвести до витоку інформації, втрати даних або несанкціонованого доступу. По-друге, кінцеві точки часто виступають першою мішенню для кібератак. Зламані пристрої можуть бути використані для подальшого розповсюдження загроз у внутрішній мережі. По-третє, безперервність бізнес-процесів організації напряму залежить від стабільної роботи кінцевих точок. Інциденти безпеки, що виводять з ладу ці пристрої, можуть спричинити збої в роботі та негативно вплинути на продуктивність компанії.

Системи управління інцидентами безпеки, такі як TheHive 5, відіграють ключову роль у забезпеченні ефективного виявлення та реагування на загрози на кінцевих точках. TheHive 5 − це платформа з відкритим кодом, яка дозволяє централізовано управляти кіберінцидентами, інтегрувати дані з інших джерел, а також автоматизувати процеси реагування за допомогою сумісності з такими інструментами, як Cortex.

TheHive 5 дозволяє фахівцям з безпеки аналізувати інциденти у структурованому вигляді, створювати кейси, документувати хід розслідування та координувати дії команди реагування. Завдяки гнучкості та модульності, система забезпечує зручну організацію роботи з інцидентами, дозволяє швидко реагувати на події безпеки, а також приймати обґрунтовані рішення щодо подальших дій.

Використання TheHive 5 дає змогу автоматизувати ключові аспекти обробки інцидентів, у тому числі класифікацію, пріоритезацію та ескалацію. Таким чином, поєднання засобів моніторингу з TheHive 5 дозволяє організаціям побудувати ефе-

ктивну систему управління інцидентами безпеки на кінцевих точках, що підвищує загальний рівень кіберзахисту.

Вищесказане визначає актуальність теми даної кваліфікаційної роботи, основний зміст якої становить дослідження методів виявлення та реагування на інциденти безпеки в кінцевих точках організації за допомогою системи TheHive 5.

Об'єкт дослідження – процес виявлення та реагування на інциденти безпеки в кінцевих точках організації.

Предмет дослідження – методи та засоби виявлення та реагування на інциденти безпеки в кінцевих точках організації на базі TheHive 5.

Мета роботи – розробити рекомендації щодо виявлення та реагування на інциденти безпеки в кінцевих точках організації на базі TheHive 5.

Наукові завдання:

дослідити актуальність проблеми виявлення та реагування на інциденти безпеки в кінцевих точках організації;

проаналізувати підходи до виявлення та реагування на інциденти безпеки в кінцевих точках організації;

проаналізувати існуючі рішення для виявлення та реагування на інциденти безпеки в кінцевих точках організації;

проаналізувати методи та засоби виявлення та реагування на інциденти безпеки кінцевих точок організації на базі TheHive 5;

розробити порядок виявлення та реагування на інциденти безпеки в кінцевих точках організації на базі TheHive 5;

розробити рекомендації щодо виявлення та реагування на інциденти безпеки в кінцевих точках організації.

Методи дослідження – аналіз літературних джерел, технічної документації та міжнародних стандартів у сфері кібербезпеки, порівняльний аналіз функціональних можливостей рішень.

Практичне значення одержаних результатів – розроблено рекомендації щодо виявлення та реагування на інциденти безпеки в кінцевих точках організації.

1. ДОСЛІДЖЕННЯ ПРОБЛЕМИ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ БЕЗПЕКИ В КІНЦЕВИХ ТОЧКАХ ОРГАНІЗАЦІЇ

1.1. Актуальність проблеми виявлення та реагування на інциденти безпеки в кінцевих точках організації

За даними звіту Unit 42 Incident Response Report [1] актуальність проблеми виявлення та реагування на інциденти безпеки в кінцевих точках організацій постійно зростає. Почали змінюватись тактики зловмисників, які дедалі частіше експлуатують технічні вразливості замість традиційних методів.

У 2023 році почалося масштабне використання вразливостей у 39% випадків. Зловмисники продовжують викрадати та використовувати скомпрометовані облікові дані. Замість ретельного відбору даних, вони швидко збирають якомога більше, викрадають їх та сортують. Іноді крадіжка даних автоматизована, разом з використанням вразливостей. Такий підхід також узгоджується з тенденцією зловмисників викрадати дані на більш ранніх етапах атаки, ніж у попередні роки.

Сучасні кіберзагрози демонструють помітну еволюцію у стратегіях проникнення до систем. Зокрема, змінюються способи отримання первинного доступу, що вказує на зростання технічної складності атак.

У 2023 році значно зросло використання вразливостей у програмному забезпеченні та API – на ці методи припало 38,6% усіх випадків початкового доступу, тоді як у 2022 році цей показник становив 28,2%. Таке значне зростання вказує на те, де зловмисники зосереджують свої зусилля.

Паралельно з цим, суттєво зросло використання скомпрометованих облікових даних – з 12,9% до 20,5% за 2022-2023 рр. У порівнянні з 2021 роком цей показник збільшився більш ніж у п’ять разів.

Фішинг поступово втрачає позиції – з 33% у 2022 році його частка знизилась до 17% у 2023-му. Таке зниження сигналізує про низьку пріоритетності фішингу, оскільки кіберзлочинці адаптуються до більш технологічно просунутих та ефективніших методів проникнення (рисунок 1.1) [1].

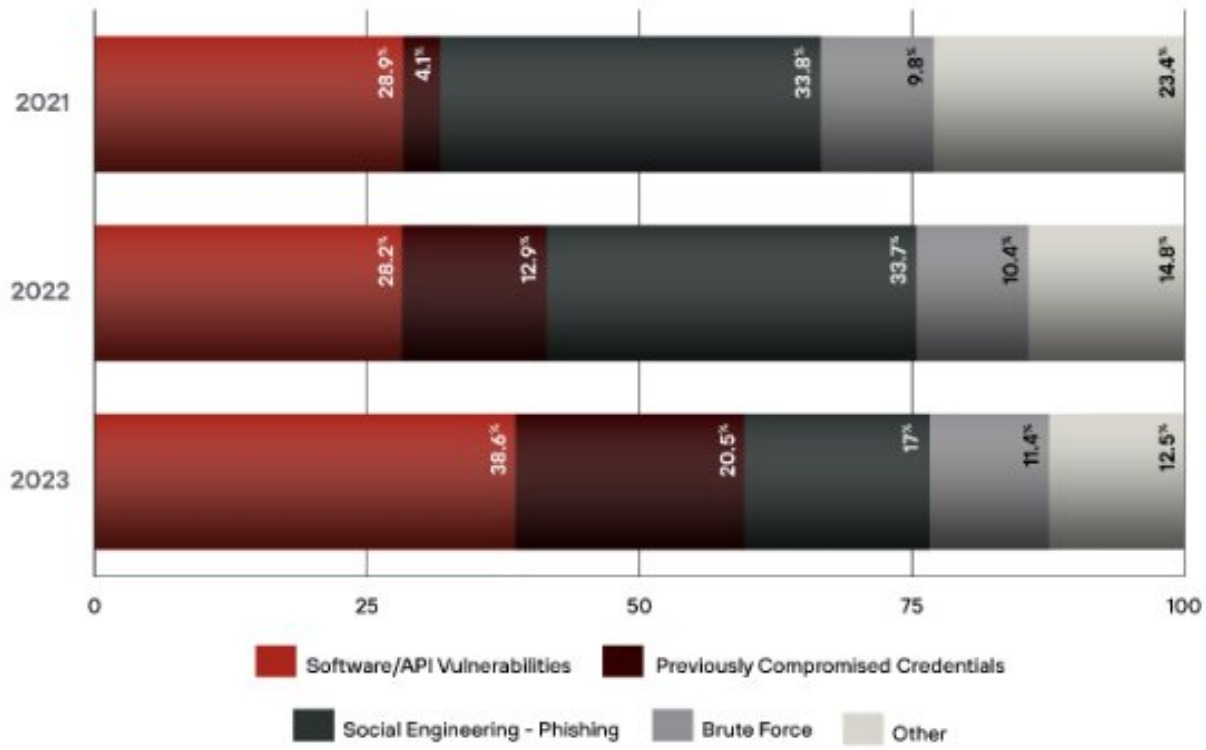

Рис. 1.1. Основні інциденти безпеки в організаціях [1]

Варто зазначити, що Україна вже тривалий час перебуває в зоні підвищеного кіберризику. Так у грудні 2015 року відбулася перша в світі успішна кібератака BlackEnergy на енергомережу, а саме на організації «Прикарпаттяобленерго», «Київобленерго» та «Чернівціобленерго», яка призвела до відключення електроенергії для 225 тисяч споживачів України [2].

2017 рік запам’ятався масштабною атакою NotPetya, що почалася із зараження українського програмного забезпечення M.E.Doc і швидко поширилася світом, завдаючи мільярдних збитків та паралізуючи роботу компаній у різних секторах [3].

У 2022 році Україна зазнала понад 2 тисячі кіберінцидентів, багато з яких були спрямовані на державні структури та критичну інфраструктуру. Зловмисники використовували шкідливе програмне забезпечення, фішинг і експлуатацію вразливостей, зокрема деструктивні віруси WhisperGate і HermeticWiper. Ці інциденти стали ключовим елементом гібридної війни, що супроводжувала повномасштабне вторгнення Росії [4].

Варто згадати про інцидент, який стався у грудні 2023-го з найбільшим мобільним оператором України – «Київстар». Тоді було зруйновано близько 70% віртуальної інфраструктури компанії. Через це мільйони абонентів тимчасово залишилися без зв’язку та інтернету, постраждали системи оповіщення і банківські сервіси. Відновлення тривало кілька днів за участі міжнародних партнерів, а «Київстар» виділив близько $90 млн на ремонт і підвищення кібербезпеки [5].

А за минулий рік Україна пережила низку потужних кібератак, які боляче вдарили по критичній інфраструктурі. У січні 2024-го Львів залишився без тепла й гарячої води у понад 600 будинках через шкідливе програмне забезпечення FrostyGoop, що проникло у систему теплопостачання через вразливість у маршрутизаторі Mikrotik. У той самий період «Нафтогаз України» зазнав атаки, внаслідок чого збої вразили офіційні сайти та сервіси, зокрема ТОВ «Газорозподільні мережі України» [6][7].

Таким чином, підтверджується актуальність своєчасного виявлення та оперативного реагування на інциденти безпеки в кінцевих точках, адже саме такі процеси є критичними для мінімізації шкоди від сучасних кіберзагроз.

1.2. Аналіз підходів щодо виявлення та реагування на інциденти безпеки в кінцевих точках організації

Одним із пріоритетних завдань забезпечення інформаційної безпеки в сучасних організаціях є своєчасне виявлення інцидентів безпеки та ефективне реагування на них. Зважаючи на високий рівень динамічності кіберзагроз, особливої уваги набуває захист кінцевих точок, які виступають одними з основних об’єктів атак. Виявлення ознак компрометації та координація заходів реагування потребують впровадження комплексного підходу, що охоплює безперервний моніторинг, аналіз аномальної активності та організацію процедур реагування. У цьому розділі наведено основні підходи до виявлення та реагування на інциденти безпеки в межах функціонування інформаційних систем організацій з урахуванням особливостей їх застосування на рівні кінцевих точок.

Функція виявлення (Detect) охоплює здатність організації вчасно ідентифікувати ознаки компрометації систем. Застосовуються такі методи [8]:

Безперервний моніторинг. Моніторинг активів для виявлення аномалій, індикаторів компрометації та інших потенційно несприятливих подій.

Аналіз аномалій і подій. Аномалії, індикатори компрометації та інші потенційно несприятливі події аналізуються для характеристики подій та виявлення інцидентів кібербезпеки.

Функція реагування (Respond) включає методи, що вживаються при підтвердженні інцидентів безпеки, зокрема [8]:

Управління інцидентами. Передбачає управління реагуванням на виявлені інциденти безпеки.

Аналіз інцидентів. Розслідування проводяться для забезпечення ефективного реагування на інциденти безпеки.

Звітність про інциденти та комунікація. Діяльність з реагування координується з внутрішніми та зовнішніми зацікавленими сторонами відповідно до вимог законів, нормативних актів або політики.

Пом'якшення наслідків інциденту. Діяльність, спрямована на запобігання поширенню події та пом'якшення її наслідків.

У контексті забезпечення кібербезпеки кінцевих точок організації важливим елементом ефективного виявлення та реагування на інциденти безпеки є наявність чітко визначених політик, планів і процедур.

Політика визначає загальні принципи та очікування щодо того, як організація має реагувати на кіберінциденти. Вона охоплює [9]:

роль і відповідальність керівництва;

типи інцидентів, що підлягають реєстрації та реагуванню;

пріоритетність або рейтинг серйозності інцидентів безпеки;

показники ефективності;

вимоги до звітності та ескалації.

План деталізує стратегію виявлення та реагування після інцидентів, особливо вразливих до атак кінцевих точок. Він передбачає [9]:

мету;

стратегії та цілі;

схвалення керівництва;

організаційні підхідоди реагування на інциденти безпеки;

оцінювання спроможності реагування на інциденти та його ефективності;

план дій розвитку спроможності реагування на інциденти безпеки;

як програма вписується в загальну структуру організації.

Процедури важливі для ефективної системи виявлення та реагування на інциденти безпеки в організації. Вони відображають пріоритети організації та визначають чіткий послідовний набір дій для усіх учасників процесу виявлення та реагування, що мінімізує ймовірність помилок, особливо в умовах підвищеної напруженості та терміновості, які характерні для інцидентних подій [9].

Для ефективного управління інцидентами безпеки в кінцевих точках організації слід чітко розуміти та впроваджувати послідовні етапи процесу реагування. До таких етапів належать (рисунок 1.2.) [9]:

підготовка;

виявлення;

аналіз;

стримування;

ліквідація та відновлення;

дії після інциденту.

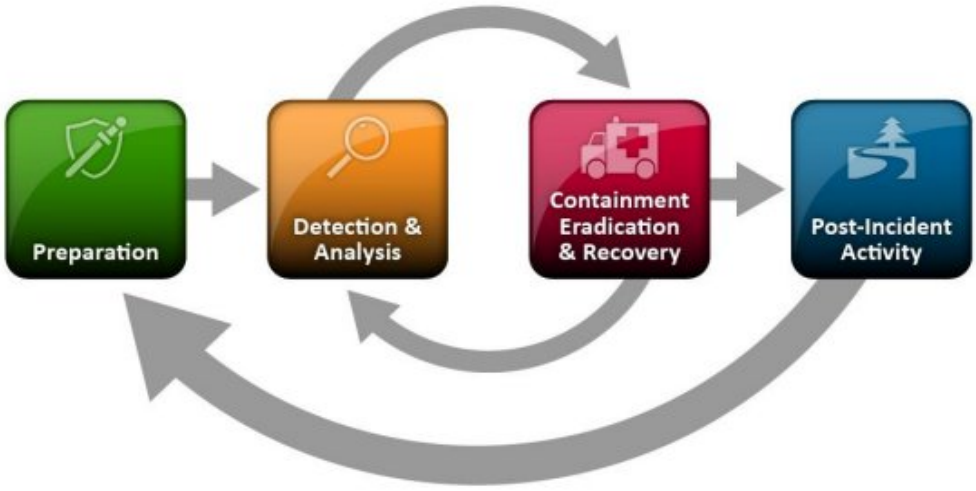

Рис 1.2. Життєвий цикл реагування на інциденти [9]

Підготовка (Preparation). Без належної підготовки будь-який наступний процес реагування на інциденти буде дезорганізований і потенційно може погіршити інцидент. Одним із найважливіших компонентів підготовки є створення плану. Після того, як буде створено план із необхідним персоналом, потрібно переконатися, що персонал, який виконує обов'язки реагування на інциденти, пройшов належну підготовку. Це включає процеси, процедури та будь-які додаткові інструменти, необхідні для розслідування інциденту. На додаток до плану слід придбати такі інструменти, як апаратне та програмне забезпечення, і включити їх у загальний процес. Також слід проводити регулярні навчання, щоб переконатися, що організація навчена та знайома з процесом [9].

Виявлення (Detection). Фаза виявлення є початковим етапом реагування на інциденти, коли організація вперше фіксує підозрілі події, які можуть свідчити про зловмисну активність. Такі події аналізуються і класифікуються як інциденти безпеки. Для прикладу, аналітик може отримати сповіщення про використання облікового запису адміністратора в період його відсутності. Інформація про потенційний інцидент безпеки також може надходити від співробітників, які помічають аномалії у роботі систем або підозрілі зміни в файлах. У кожному з таких випадків організація має оцінити ситуацію, підтвердити інцидент та розпочати відповідні заходи реагування для розслідування і нейтралізації загрози [9].

Аналіз (Analysis). Після виявлення інциденту відповідальні працівники організації або уповноважена третя сторона переходять до фази аналізу. На цьому етапі збираються докази з різних джерел, як оперативна пам’ять, лог-файли, мережеві з’єднання та запущені процеси програмного забезпечення.. Тривалість збору даних може варіюватися від кількох годин до кількох днів залежно від характеру інциденту. Коли докази зібрано, проводиться їх детальне дослідження за допомогою спеціалізованих інструментів, що дозволяють встановити, що саме сталося, які системи були уражені, чи було скомпрометовано конфіденційні дані, а також чи поширилася загроза на інші об’єкти. Основною метою аналізу є виявлення першопричини інциденту безпеки та відтворення послідовності дій зловмисника від моменту проникнення до моменту виявлення інциденту [9].

Стримування (Containment). Коли встановлено характер інциденту безпеки та визначено уражені системи, організація переходить до фази стримування. Метою цього етапу є зупинити подальше поширення загрози, запобігти витоку конфіденційних даних та обмежити взаємодію з інфраструктурою управління зловмисника. Залежно від ситуації, стримування може включати блокування IP-адрес і портів на брандмауері або фізичне від’єднання зараженого пристрою від мережі. Вибір стратегії залежить від типу інциденту, а наявність кількох підходів підвищує шанси ефективного стримування загрози до того, як буде завдано значної шкоди [9].

Ліквідація та відновлення (Eradication and Recovery). Під час фази ліквідації організація усуває загрозу з уражених систем. Якщо виявлено шкідливе програмне забезпечення, застосовуються спеціалізовані засоби для його видалення. У складніших випадках заражені пристрої можуть бути очищені або відновлені за допомогою повторної інсталяції операційної системи та програмного забезпечення. Також проводиться деактивація або зміна скомпрометованих облікових записів користувачів. У разі виявлення використаної вразливості, організація впроваджує відповідні оновлення або патчі. Діяльність з ліквідації тісно пов’язана з планами безперервності бізнесу та аварійного відновлення, оскільки включає відновлення даних із резервних копій та перевірку безпеки облікових записів. На завершення проводиться повне сканування систем для виявлення і усунення потенційних вразливостей.

Діяльність після інциденту (Post-Incident Activity). Завершальним етапом реагування на інцидент є діяльність після інциденту, що включає ретельний аналіз усіх дій, вжитих під час інциденту безпеки. Обговорюються як ефективні рішення, так і ті, що не спрацювали. На основі цього формується письмовий звіт, який фіксує хронологію подій, виявлену першопричину та ключові висновки. Зрештою, персонал організації має переглядати та вдосконалювати власні процедури реагування на інциденти, враховуючи нову інформацію, отриману під час аналізу та підсумкової звітності. Урахування цих висновків є ключовим для підвищення ефективності дій під час майбутніх інцидентів.

Оперативне виявлення та реагування на інциденти в кінцевих точках мінімізує ризики і швидко відновлює роботу систем. Постійне вдосконалення процесів забезпечує організації готовність до нових кіберзагроз.

1.3. Аналіз рішень щодо виявлення та реагування на інциденти безпеки в кінцевих точках організації

У наш час організації стикаються з численними інцидентами безпеки, які можуть виникати без попередження та швидко поширюватися через кінцеві точки. Ефективне виявлення та реагування на інциденти дозволяє не лише своєчасно їх виявляти, а й оперативно нейтралізувати, мінімізуючи потенційні збитки. Серед сучасних рішень для виявлення та реагування на інциденти безпеки в кінцевих точках варто згадати Velociraptor, InsightIDR та GRR Rapid Response.

Velociraptor – це інструмент з відкритим вихідним кодом, розроблений для контролю, моніторингу та збору даних з кінцевих точок. Він допомагає фахівцям з реагування на інциденти та криміналістам запитувати та аналізувати системи на наявність ознак вторгнення, зловмисної активності або порушень політик.

Velociraptor пропонує широкий спектр функціональних можливостей, що робить його гнучким для різних операцій з кібербезпеки [10]:

Мова запитів Velociraptor Query Language (VQL). VQL дозволяє аналітикам писати складні запити для отримання конкретних даних з кінцевих точок. Незале-

жно від того, чи аналітик аналізуєте журнали подій або шукає індикатори компрометації (IoC) на тисячах кінцевих точок, VQL абстрагує значну частину складності, дозволяючи зосередитися на даних, які мають значення.

Полювання в кінцевих точках та запити на IoC. Velociraptor унікальний інструмент для полювання на загрози у великих середовищах. Він може запитувати тисячі кінцевих точок одночасно, щоб знайти докази вторгнення, підозрілої поведінки або присутності шкідливого програмного забезпечення.

Безперервний моніторинг та реагування. За допомогою Velociraptor можна налаштувати безперервний моніторинг певних системних подій, таких як створення процесів або невдалі входи в систему. Дозволяє командам безпеки відстежувати незвичну або зловмисну активність у режимі реального часу та швидко реагувати.

Запити на колекції та запити на події. Velociraptor використовує два типи запитів VQL - запити на колекції, що виконуються один раз і повертають результати на основі поточного стану системи, та запити на події, які безперервно запитують і передають результати при виникненні нових подій, що робить їх ефективними для моніторингу поведінки системи в часі.

Інтеграція зі сторонніми рішеннями. Для додаткового збору та аналізу Velociraptor може інтегруватися зі сторонніми інструментами, що розширює його можливості в більш спеціалізованих сценаріях.

У Velociraptor використовується такі основні компоненти, як (рисунок 1.3) [11]:

Клієнт, який є екземпляром Velociraptor та працює на кінцевій точці, тобто це «агент» кінцевої точки.

Фронтенд (сервер) – серверний компонент, який взаємодіє з клієнтом.

Графічний інтерфейс користувача (GUI) є сервером веб-застосунків, який забезпечує адміністративний інтерфейс.

Прикладний програмний інтерфейс (API) представлений як сервер API на основі gRPC.

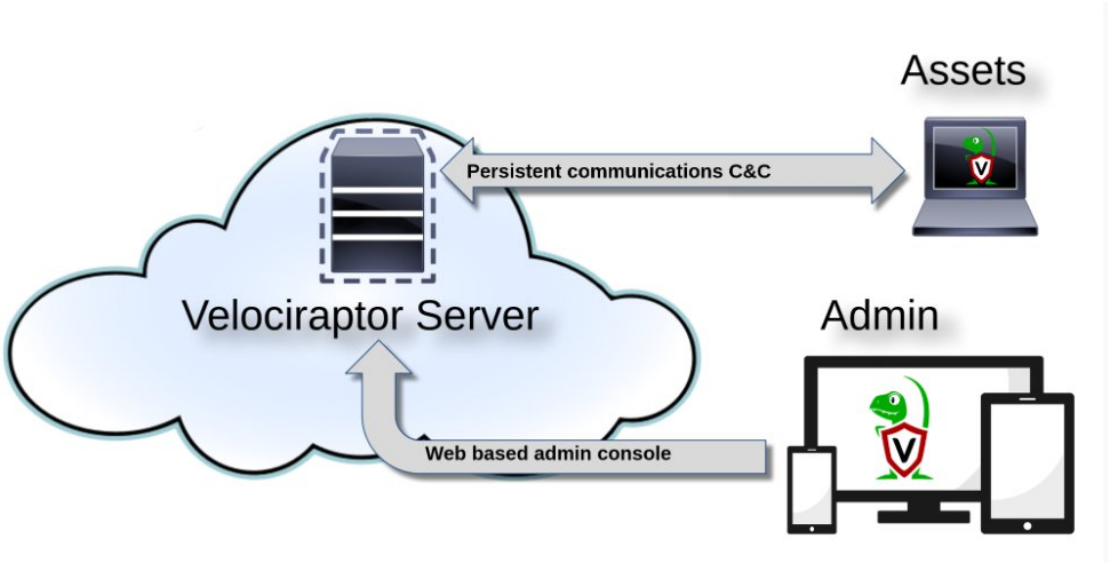

Рис. 1.3. Архітектура та компоненти Velociraptor [11]

InsightIDR є хмарним рішенням для виявлення загроз, реагування на інциденти безпеки. Воно забезпечує централізований моніторинг безпеки, включаючи контроль автентифікації, відстеження активності користувачів і захист кінцевих точок. InsightIDR допомагає швидко виявляти підозрілу поведінку та несанкціонований доступ, зменшуючи обсяг ручної перевірки даних завдяки автоматизованому аналізу та інтеграції різних джерел інформації [12].

Ключовими особливостями InsightIDR є [12]:

Об'єднання даних для єдиного огляду безпеки. InsightIDR збирає дані з різних джерел, таких як мережеві ресурси, пристрої користувачів та хмарні сервіси, нормалізує їх та прив'язує до конкретних користувачів, що забезпечує чітке розуміння походження, власника та часу події.

Аналіз логів, даних кінцевих точок та мережевого трафіку. InsightIDR збирає потоки даних з усіх можливих місць і об'єднує їх в одному зручному для аналізу місці.

Отримання сповіщень про підозрілу активність. Незалежно від того, чи відбувається у мережі підозріла активність, InsightIDR встановлює заходи, які сповіщають про прогалини в безпеці.

Пріоритетність подій. Завдяки нормалізації даних, InsightIDR автоматично пріоритизує мережеві події та виділяє важливі інциденти, фільтруючи некритичні події.

Розслідування подій. У разі порушення безпеки, команди безпеки отримують контекстну інформацію про скомпрометовані дані, час події та можливі подальші дії зловмисника, що полегшує розслідування інцидентів безпеки.

Моніторинг діяльності операцій безпеки. Панель керування активністю операцій безпеки синтезує дані в дієві відомості, полегшуючи реагування на сповіщення, звітування про тенденції загроз та аналіз ефективності команди безпеки.

Архітектура InsightIDR включає такі основні компоненти (рисунок 1.4) [12]:

колектор;

агент;

мережевий сенсор;

оркестратор;

хмарне середовище.

Рис. 1.4. Архітектура та компоненти InsightIDR [12]

Колектор (Insight Collector) є локальним компонентом InsightIDR, який виконує роль локального агента для збору, обробки та передачі логів та інших даних безпеки до хмарної платформи для подальшого аналізу [13].

Робочий процес колектора має дві основні переваги порівняно з безпосереднім надсиланням логів до InsightIDR [13]:

Нормалізація. Нормалізація перетворює дані в логах з різних джерел у загальний формат JSON і витягує стандартну інформацію, таку як імена хостів, часові мітки та рівні помилок. Вона дозволяє виконувати більш складні запити до логів кінцевих точок і покращує візуалізацію даних.

Атрибуція користувачів. Атрибуція користувачів пов'язує активність кінцевого пристрою з окремими користувачами, які використовують цей пристрій під час входу в додатки. Атрибуція дає більш повне уявлення про систему безпеки, оскільки облікові записи користувачів є найпоширенішими цілями для складних атак.

Механізм дедуплікації даних (Data Deduplication) в колекторі забезпечує високоякісний, структурований і оптимізований для аналізу потік даних. Дедуплікація об'єднує повторювані події в єдині записи, що зменшує обсяг збережених даних та прискорює пошук, зберігаючи при цьому точність підрахунку кількості повторів активності через поля [13]

observation_count – показує, скільки разів однакова активність була виявлена при обробці отриманих даних. Методика збору даних InsightIDR групує кілька рядків або подій з одного джерела подій разом для обробки, і дедуплікація відбувається в цих групах подій.

first_observed_time – показує дату та час першого дубліката запису лога, що міститься в групі подій.

last_observed_time – показує дату та час останнього дубліката запису лога, що міститься в групі подій.

Такі поля присутні лише в тих подіях, де одна і та ж активність відбулася кілька разів у групі подій.

Агент (Insight Agent) має вирішальне значення для здатності InsightIDR забезпечувати виявлення та реагування на кінцеві точки в режимі реального часу, що необхідно для виявлення ранніх ознак атаки. Він функціонує як легке програмне забезпечення, яке можна встановити на підтримуваних ресурсах, у хмарних або локальних середовищах [15].

Агент надає користувачам InsightIDR кілька переваг, зокрема [14]:

Виявлення на ранніх етапах ланцюга атаки. Агент дозволяє виявляти підозрілу активність на ранніх етапах атаки, забезпечуючи безперервний моніторинг автентифікацій, процесів, що виконуються, та активності користувачів на підтримуваних пристроях.

Доступ до спеціалізованих правил виявлення. Агент надає можливість застосовувати сотні виявлення для аналітики зловмисників, які залежать від даних про запущені процеси. Правила дозволяють своєчасно виявляти підозрілу поведінку, пов'язану з тактиками та техніками зловмисників.

Перегляд ресурсів, запущених із віддалених місць. Може контролювати пристрої, які перебувають поза межами корпоративної мережі, а також забезпечити повну видимість, коли ресурси підключаються до інтернету з інших локацій.

Ізоляція скомпрометованих користувачів та ресурсів. Дає змогу користувачам InsightIDR швидко реагувати на інциденти безпеки в кінцевих точках шляхом автоматичної ізоляції скомпрометованих користувачів та ресурсів, що виявляють підозрілу активність.

Використання технологій обману (deception) у кінцевих точках. Агент підтримує функцію Honey Credentials для заманювання хакерів за допомогою доступних облікових даних на підтримуваних ресурсах.

Моніторинг цілісності файлів (FIM). За допомогою FIM можна відстежувати зміни у важливих файлах і папках. Агент напряму прив'язує події змін до конкретних користувачів, що сприяє точному і швидкому проведенню аудиту та розслідуванню.

Легке завантаження. На відміну від багатьох інших агентів, агент у InsightIDR має малий розмір та низьке споживання ресурсів. Його просто встановити, а робота системи залишається стабільною без надмірного навантаження на CPU або диск.

Мережевий сенсор (Insight Network Sensor) може здійснювати моніторинг, захоплення та оцінку наскрізного мережевого трафіку, що проходить через фізичну та віртуальну інфраструктуру. Рішення Insight можуть використовувати дані цього мережевого сенсора для своїх конкретних випадків використання [15].

Існує три варіанти розгортання мережевого сенсора. Ці варіанти пропонують видимість мережевого трафіку, але розгортаються та налаштовуються по-різному [15]:

розгортання на фізичному сервері;

розгортання на віртуальній машині;

розгортання у середовищі AWS з використанням EC2.

У таблиці 1.1. наведено відомості для кожного варіанта розгортання [15].

Таблиця 1.1. [15]

Варіанти розгортання мережевого сенсора

Фізичний сервер	Віртуальна машина	Віртуальна приватна хмара AWS (VPC)
Розгорнуто на виділеному фізичному сервері	Розгорнуто як віртуальна машина на сервері VMWare ESX	Розгорнуто на екземплярі EC2
Підключається до групи портів, SPAN або дзеркального порту	Підключається до групи портів, SPAN або дзеркального порту	Отримує трафік AWS Mirror
Підходить для аналізу високошвидкісного трафіку, 1,5 Гбіт/с або більше	Підходить для швидкого налаштування, перевірки концепції або якщо потрібна видимість зі сходу на захід у віртуальних середовищах	Підходить для видимості трафіку зі сходу на захід та з півночі на південь у межах віртуальних торгових центрів AWS

Хмарне середовище (Insight Cloud) існує як хмарна платформа для управління безпекою, яка об’єднує різні інструменти для виявлення, аналізу та реагування на інциденти безпеки.

У рамках функціонування хмарної платформи Insight Cloud не застосовуються стандартні методи збору даних. Натомість здійснюється ідентифікація автентифікаційних облікових даних, доменів, токенів, ключів доступу та різноманітних типів ідентифікаторів відповідно до специфіки джерела подій. Після підключення джерела подій хмарного сервісу можна окремо відсте-жувати автентифікаційну активність у хмарі через вікно Ingress Locations, яке відображається на інформа-

ційній панелі InsightIDR. Оскільки дані надходять безпосередньо від хмарного середовища, InsightIDR забезпечує збір і візуалізацію інформації про доступ до сервісу з будь-якої локації – як з внутрішньої корпоративної мережі, так і з зовнішніх середовищ.

InsightIDR визначає користувачів із правами адміністратора хмарного сервісу на основі аналізу їхньої активності, зафіксованої у результатах пошуку журналів, без використання попередньо заданих списків API або порівняння з зовнішніми системами керування доступом. Платформа аналізує записи логів, що надходять із підключених джерел подій, та відстежує характерні дії в хмарному середовищі, які свідчать про наявність адміністративного доступу [16].

Оркестратор (Insight Orchestrator) являє собою сервер, розгорнутий у внутрішньому середовищі або хмарі, який забезпечує виконання автоматизованих дій у рамках заздалегідь визначених робочих процесів.

Під час виконання робочого процесу хмарне середовище (Insight Cloud) зберігає як загальну логіку його виконання, так і дані, що генеруються на кожному етапі. Якщо окремий крок налаштований для виконання через оркестратор, система передає йому вхідні дані разом із відповідними інструкціями. Оркестратор виконує задану дію та повертає результати назад до хмарного середовища, після чого переходить до наступного етапу процесу. Облікові дані, що використовуються у встановлених з'єднаннях, шифруються безпосередньо в оркестраторі, забезпечуючи додатковий рівень безпеки [17].

Оркестратор розроблено для безпечного зв'язку із хмарним середовищем та безпечного зберігання конфіденційних конфігурацій з'єднання, включаючи облікові дані. Кожен оркестратор генерує дві пари закритих та відкритих ключів для зв'язку з хмарою [17]:

перша пара облікових даних призначена для шифрування та розшифрування облікових даних;

друга пара облікових даних призначена для загальних підписів еліптичних кривих для підписання та перевірки запитів.

Оркестратор регулярно встановлює зв’язок із хмарним сервісом. Комунікація завжди ініціюється лише з боку оркестратора, а хмара не має змоги самостійно звертатися до оркестратора, встановленого у інфраструктурі.

Наведено основні випадки взаємодії оркестратора з хмарним середовищем [17]:

Сигнали активності (heartbeat data). Оркестратор періодично надсилає сигнали, що підтверджують його працездатність і готовність до обробки завдань. Ці сигнали містять метадані про його стан, що дозволяє системі підтримувати працездатність. У відповідь оркестратор отримує токен, який надалі використовується для підпису запитів. Без надсилання цих сигналів подальша взаємодія з хмарою неможлива.

Запити на виконання завдань. Оркестратор ініціює безпечне з’єднання із використанням зашифрованого каналу для отримання нових завдань, які включають метадані про нього для його ідентифікації в хмарі. Такі запити підписуються та перевіряються.

Передача результатів. Після виконання завдань оркестратор надсилає результати до хмари. Як і запити, ці повідомлення також підписуються та перевіряються.

Кожен оркестратор має картку (Orchestrator card), які виконують роль інформаційної панелі. Картки відображають дані оркестратора, а також дозволяють переглядати стан оркестратора або видаляти будь-які за потреби.

Картка кожного оркестратора містить [17]:

загальну кількість подій;

кількість подій, що обробляються на даний момент;

кількість підключень;

використання процесора;

використання пам’яті у байтах;

використання сховища у байтах.

GRR Rapid Response – це система реагування на інциденти безпеки, орієнтована на розслідуванні в реальному часі [18].

GRR складається з двох частин [18]:

Клієнтська. Розгортається на системах, які, можливо, варто дослідити. У кожній такій системі, після розгортання, клієнт GRR періодично опитує фронтенд-сервери GRR на предмет роботи. «Робота» означає виконання певної дії – завантаження файлу, перегляд каталогу тощо.

Серверна. Складається з кількох компонентів (фронтенди, воркери, сервери інтерфейсу користувача, fleetspeak) та надає графічний веб-інтерфейс користувача й кінцеву точку API, що дозволяє аналітикам планувати дії на клієнтах, а також переглядати та обробляти зібрані дані.

Особливостями GRR є [18]:

Кросплатформеність. Підтримує клієнтів на Linux, macOS та Windows.

Аналіз віддаленої пам'яті в режимі реального часу. Використовує бібліотеки YARA для виявлення шкідливих шаблонів у оперативній пам'яті.

Потужні можливості пошуку та завантаження файлів. Доступ до файлової системи для збору артефактів.

Повноцінне реагування на інциденти. Дозволяє виконувати більшість завдань реагування на інциденти безпеки.

Швидкий збір артефактів. Просте отримання сотень об'єктів розслідування.

Моніторинг ресурсів. Детальний контроль використання CPU, пам'яті, а також встановлення обмежень.

Асинхронна обробка. Асинхронний дизайн, що дозволяє планувати завдання для клієнтів наперед, що зручно для управління численними пристроями.

GRR складається з клієнта та кількох серверних компонентів. При встановленні GRR сервера одним із зазначених способів усі серверні компоненти інсталюються одночасно. Для невеликих розгортань це найпростіший варіант, кожен компонент запускається як окремий серверний процес на одній машині. Проте для масштабування системи GRR компоненти можуть бути розподілені по різних серверах у дата-

центрі і працювати незалежно один від одного, що забезпечує більшу продуктивність та стійкість [19].

Компоненти GRR (рисунок 1.5.) [19]:

клієнт;

сховище даних;

сервер Fleetspeak;

адміністративний сервер Fleetspeak;

база даних Fleetspeak;

фронтальні сервери;

робочі компоненти (worker);

веб-інтерфейс.

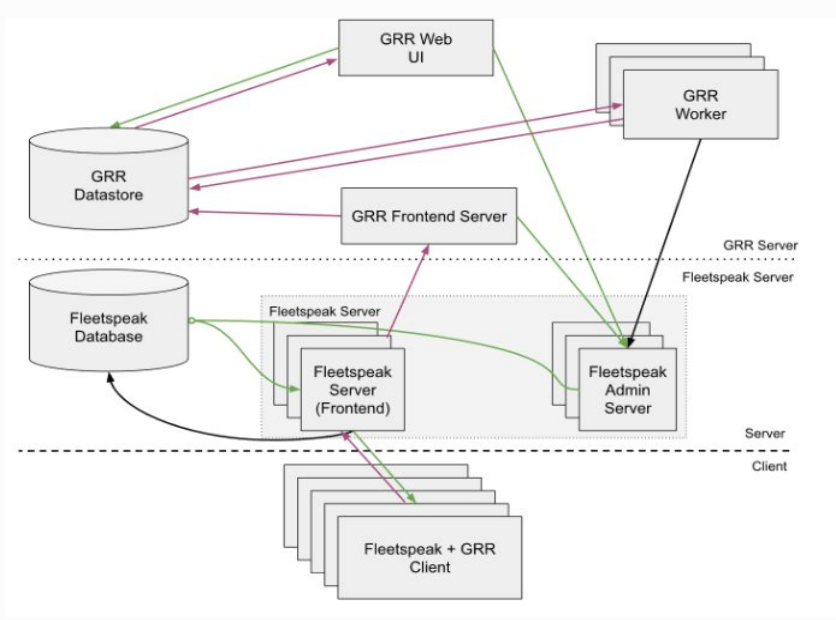

Рис. 1.5. Компоненти GRR Rapid Response [19]

Клієнт. Не входить до складу серверних компонентів, однак постачається разом із сервером у складі дистрибутиву. Його розгортання на корпоративних пристроях здійснюється стандартними засобами управління програмним забезпеченням. Клієнт складається з 2 процесів, а саме клієнт fleetspeak, який відповідає за реалізацію протоколу зв'язку на основі потокового HTTPS-з'єднання. Процес клієнта GRR надсилає та отримує повідомлення GRR від сервера та реалізує бізнес-логіку [19].

Сховище даних. Діє як центральний компонент зберігання даних, так і як механізм зв'язку для всіх компонентів сервера GRR [19].

Сервер Fleetspeak. Відповідає за підтримку потокових HTTPS-з'єднань від клієнтів Fleetspeak та реалізацію протоколу обміну даними. Він приймає повідомлення від клієнтів і доставляє їм повідомлення, що знаходяться у черзі на відправку [19].

Адміністративний сервер Fleetspeak. Надає інтерфейс для надсилання повідомлень клієнтам з GRR-сервера [19].

База даних. Система fleetspeak використовує базу даних MySQL для організації черги повідомлень для клієнтів [19].

Фронтальні сервери. Основною функцією фронтальних серверів є приймання повідомлень GRR від сервера Fleetspeak, їх розбір на окремі повідомлення та передача у чергу для зберігання в сховищі даних. Крім того, фронтенд відповідає за отримання повідомлень, що очікують на відправлення клієнту, і передачу їх відповідному клієнтському агенту [19].

Робочі компоненти *(worker)*. Для забезпечення масштабованості фронтенд не виконує обробку даних самостійно, а делегує її спеціалізованим робочим компонентам (workers). Кількість таких компонентів може бути адаптована відповідно до зростання навантаження. Вони регулярно опитують черги в сховищі даних на наявність відповідей від клієнтів, обробляють отримані дані та формують нові запити, які потім ставляться в чергу для подальшого надсилання клієнтам [19].

Веб-інтерфейс. Існує в GRR основним інструментом взаємодії з системою для спеціалістів з реагування на інциденти та цифрової криміналістики. Через нього аналітики можуть призначати завдання для клієнтів, переглядати результати раніше виконаних операцій, а також контролювати хід розслідування [19].

Проведений аналіз не лише дозволив оцінити ефективність існуючих рішень, як Velociraptor, InsightIDR та GRR Rapid Response, а й відкрити можливості для ефективного виявлення та реагування на інциденти в кінцевих точках організації.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ БЕЗПЕКИ В КІНЦЕВИХ ТОЧКАХ ОРГАНІЗАЦІЇ НА БАЗІ THEHIVE 5

2.1. Призначення та основні функції рішення TheHive 5

У контексті сучасних підходів до виявлення та реагування на інциденти безпеки в кінцевих точках організацій, особливу увагу заслуговують платформи, які забезпечують координацію дій команд реагування та автоматизацію розслідувальних процесів. Таким є рішення TheHive 5, яке відіграє вирішальну роль у цьому. Цей розділ присвячено детальному аналізу можливостей TheHive 5 у контексті кібербезпеки, його ролі в процесах виявлення та реагування на інциденти безпеки, а також його взаємодії з іншими інструментами.

TheHive 5 – комплексна відкрита платформа для реагування на інциденти інформаційної безпеки, яка представлена ключовим інструментом для команд SOC, CSIRT, CERT та всіх спеціалістів з інформаційної безпеки, які беруть участь у швидкому та ефективному реагуванні на інциденти безпеки. Складається з потужного набору функцій, призначених для оптимізації робочих процесів реагування на інциденти, покращення співпраці та розширення можливостей фахівців з інформаційної безпеки ефективно розслідувати та зменшувати інциденти безпеки [20].

Дане рішення містить такі основні особливості, як [20]:

Інтеграція з MISP. Платформа тісно інтегрована з MISP, що забезпечує безперешкодний обмін інформацією та ефективну співпрацю між учасниками розслідування інцидентів.

Співпраця в режимі реального часу. TheHive 5 дозволяє декільком аналітикам одночасно працювати над інцидентами, отримуючи актуальні оновлення щодо кейсів, завдань, спостережуваних даних та IoC.

Ефективне управління завданнями. Завдяки системі сповіщень та інтеграції з джерелами, такими як електронна пошта, провайдери CTI та SIEM, завдання можуть бути оперативно створені, призначені та оброблені.

Налаштовані шаблони. Користувачі можуть створювати кейси та завдання за допомогою гнучкого механізму шаблонів, що дозволяє налаштовувати метрики і кастомні поля, щоб керувати діяльністю команди і визначати області для автоматизації.

Управління доказами. Аналітики можуть фіксувати хід розслідування, прикріплювати файли, додавати теги, а також безпечно імпортувати захищені паролем ZIP-архіви, що містять підозрілі дані.

Управління спостережуваними даними. Платформа дозволяє легко додавати та управляти спостережуваними об’єктами як індивідуально, так і масово, з можливістю імпорту безпосередньо з подій або оповіщень MISP. Функції сортування та фільтрації спрощують процес.

Інтеграція з системами розвідки загроз. Використовуючи рішення Cortex та його аналізатори, TheHive 5 забезпечує збагачення даних про загрози, прискорює розслідування та дозволяє оперативно реагувати на інциденти. Теги, IoC та інші спостережувані об’єкти можуть бути використані для покращення якості розвідки.

TheHive 5 має значні переваги порівняно з TheHive 4, які зосереджені на покращенні користувацького досвіду та безпеки [21] [22]:

Сучасний інтерфейс користувача. TheHive 5 пропонує повністю оновлений інтерфейс з можливістю налаштування списків даних, збереження власних фільтрів та вибору мови інтерфейсу.

Покращене управління сповіщеннями. Додано можливість попередньої обробки сповіщень на спостережуваних об’єктах, додавання коментарів та відображення подібних сповіщень.

Нові можливості для кейсів. Візуальна шкала часу кейсу, вкладки для коментарів, вкладення, сторінки у стилі wiki та експорт кейсів.

Інтерактивні дашборди: Створення приватних та спільних дашбордів з розширеними віджетами та ключовими показниками ефективності.

Впровадження нової концепції. TheHive 5 впроваджує нову концепцію Functions − вбудованих JavaScript-сценаріїв, які дозволяють обробляти вхідні вебхуки та виконувати дії без залучення зовнішніх сервісів, а також відкриває широкі можливості для автоматизації та інтеграції з іншими системами.

Розширене управління шаблонами кейсів. У TheHive 5 можуть застосовуватися кілька шаблонів до одного кейсу, що дозволяє динамічно додавати завдання та поля в міру розвитку розслідування.

Обов'язкові завдання. Адміністратори можуть позначати певні завдання як обов'язкові, що унеможливлює закриття кейсу без їх виконання. Аналітик не зможе закрити кейс, поки не буде додано записи до журналу для кожного з таких завдань, що гарантує підвищену якість реагування на інциденти.

2.2. Архітектура та компоненти TheHive 5

Архітектура TheHive 5 є високомодульною, що дозволяє розгортати кожен рівень (додаток TheHive, базу даних та механізм індексації, а також файлове сховище) незалежно як окремі вузли або як частину кластерної структури. Кожен із цих рівнів може бути налаштований як окремий вузол або інтегрований у кластерну інфраструктуру. Такий підхід дозволяє створювати масштабовані рішення з використанням віртуальних IP-адрес і балансувальників навантаження, що сприяє досягненню високої продуктивності та надійності системи.

До основних компонентів інфраструктури TheHive 5 належать (рисунок 2.1.) [20]:

Apache Cassandra;

Elasticsearch;

рішення для зберігання файлів (локальна файлова система або MinIO).

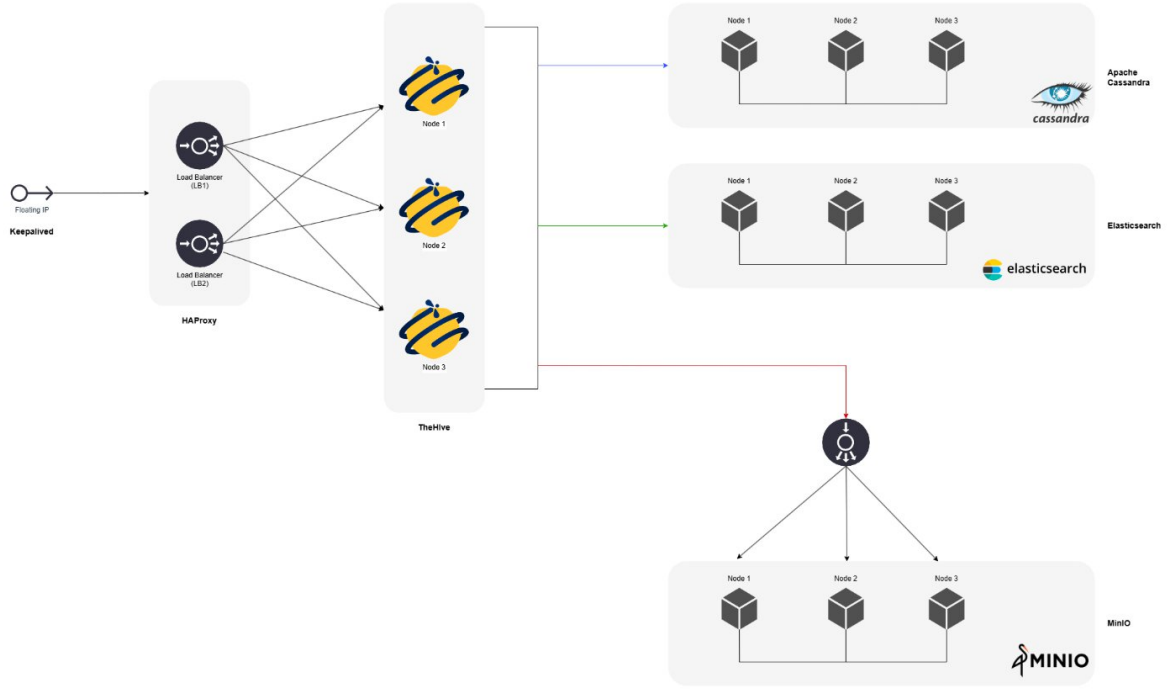

Рис. 2.1. Архітектура та компоненти TheHive 5 [20]

Огляд компонентів рішення TheHive 5

Apache Cassandra − розподілена масштабована NoSQL база даних із відкритим кодом, яка побудована за секціонованою моделлю зберігання з підтримкою широких стовпців. Вона забезпечує високу доступність, відмовостійкість і остаточну узгодженість даних у розподіленому середовищі.

Cassandra оптимізована для роботи з великими обсягами даних і високонавантаженими системами, де необхідна швидка обробка операцій читання та запису з низькою затримкою. Вона підтримує автоматичне розподілення та реплікацію даних між вузлами кластера, що забезпечує масштабування без єдиної точки відмови [23].

Cassandra надає мову запитів CQL, подібну до SQL, для створення, модифікації та видалення схеми бази даних, а також доступу до даних. CQL дозволяє користувачам організовувати дані у кластері вузлів Cassandra [23]:

Простір ключів. Визначає стратегію реплікації набору даних між різними центрами даних. Реплікація відноситься до кількості копій, що зберігаються в кластері. Простори ключів слугують контейнерами для таблиць.

Таблиця. Таблиці складаються з рядків і стовпців. Стовпці визначають типізовану схему для одного елемента даних у таблиці. Таблиці розбиваються на розділи на основі стовпців, вказаних у ключі розділу. Таблиці Cassandra можуть гнучко додавати нові стовпці до таблиць з нульовим часом простою.

Розділ. Визначає обов'язкову частину первинного ключа, яку повинні мати всі рядки в Cassandra для ідентифікації вузла в кластері, де зберігається рядок. Всі виконувані запити надають ключ розділу в запиті.

Рядок. Містить набір стовпців, ідентифікованих унікальним первинним ключем, що складається з ключа розділу і, за бажанням, додаткових ключів кластеризації.

Стовпець. Єдине джерело даних з типом, який належить до рядка.

CQL підтримує численні розширені можливості для роботи з розділеними наборами даних, такі як [23]:

типи колекцій, включаючи набори, карти та списки;

визначені користувачем типи, кортежі, функції та агрегації;

індексування з прив'язкою до сховища для вторинних індексів;

локальні вторинні індекси;

однорозрядні полегшені транзакції з атомарним порівнянням та семантикою множин

експериментальні або матеріалізовані подання.

Структура Apache Cassandra розподілена на багатьох стандартних серверах. Зазвичай вона виглядає так (рисунок 2.2) [24]:

Однорангова розподілена система. Всі вузли Cassandra в кластері рівноправні і взаємодіють один з одним без необхідності централізованого координатора, уникаючи єдиної точки відмови.

Кільцеві кластери. Структура Apache Cassandra розподіляє дані по всьому кластеру по кільцю, при цьому кожен з вузлів кластера відповідає за діапазон даних, визначений алгоритмом хешування.

Коефіцієнт реплікації даних. Cassandra реплікує файли даних між кількома вузлами і може бути налаштована в межах одного центру обробки даних або між кількома сайтами.

Модель даних. Cassandra є опційною схемою, що використовує гнучку модель зберігання даних з розділеними рядками. У ній дані зберігаються організовано в рядки на основі ключа розділу – підмножини первинного ключа або самого первинного ключа, якщо він простий.

Шляхи читання і запису. Cassandra підтримує швидкі операції запису і читання, використовуючи розподілений журнал фіксації і таблицю пам'яті для запитів на запис і розподілену операцію читання між репліками для читання.

Протокол пліток (Gossip protocol). Протокол пліток Cassandra для міжвузлової взаємодії дозволяє вузлам виявляти та обмінюватися інформацією про стан кластера та топологію мережі.

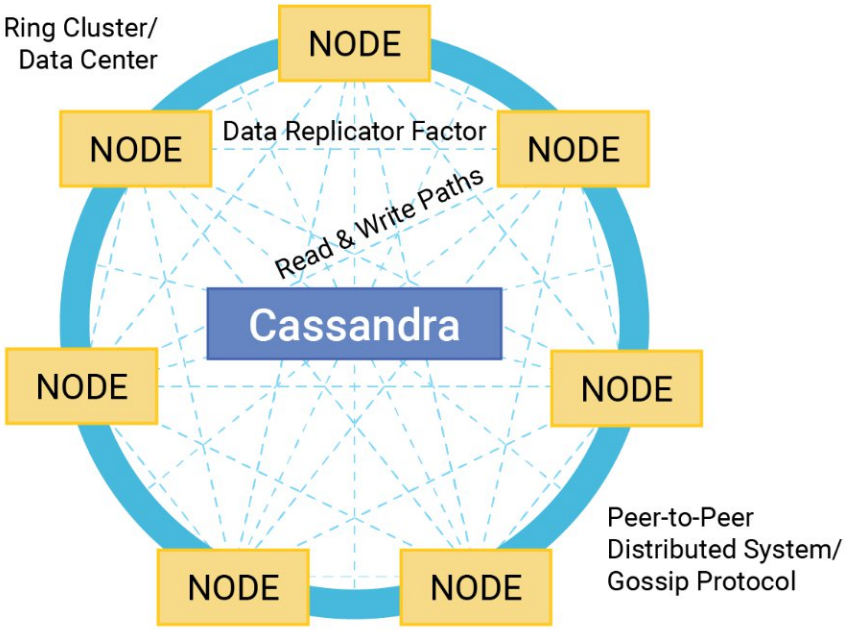

Рис. 2.2. Структура Apache Cassandra

Elasticsearch є розподіленою пошуковою та аналітичною системою, масштабоване сховище даних та векторна база даних, побудовані на Apache Lucene. Вона оптимізована для швидкості та релевантності для робочих навантажень у масштабі виробництва. Elasticsearch використовується для пошуку, індексації, зберігання та аналізу даних усіх форм і розмірів майже в режимі реального часу [25].

Особливості Elasticsearch [25]:

Повнотекстовий пошук. Створення швидкого та релевантного рішення для повнотекстового пошуку з використанням інвертованих індекси, токенів та аналіз тексту.

Векторна база даних. Зберігання та пошук векторних даних, а також створення векторних вставок за допомогою вбудованих та сторонніх моделей обробки природної мови.

Семантичний пошук. Розуміння намірів та контексту значення пошукових запитів за допомогою таких інструментів, як синоніми, щільні векторні представлення та розріджене розширення запиту.

Гібридний пошук. Поєднання повнотекстового пошуку з векторним, використовуючи найсучасніші алгоритми ранжування.

Створення можливості пошуку. Додавання гібридних можливості пошуку в додатки або веб-сайти, створення корпоративних пошукових систем на основі внутрішніх джерел даних організації.

Розширена генерація пошуку. Використання Elasticsearch як механізм пошуку для доповнення генеративних моделей штучного інтелекту більш релевантними, актуальними або власними даними для різних випадків використання.

У таблиці 2.1. наведені варіанти використання Elasticsearch [26].

Таблиця 2.1. [26]

Варіанти використання Elasticsearch

Випадок використання	Цілі	Технічні вимоги
Векторний пошук та гібридний пошук	Запуск пошуку найближчого сусіда, комбінування з	Щільні та розріджені вбудовані елементи у поєднанні з текстом

Продовження табл. 2.1.

Варіанти використання Elasticsearch

Випадок використання	Цілі	Технічні вимоги
Пошук в електронній комерції та каталогах товарів	Надання швидких, відповідних та актуальних результатів, багатогранної навігації	Синхронізація даних, відстеження поведінки користувачів, кешування результатів
Пошук по робочому місцю і на базі знань	Пошук у різних джерелах даних, застосування дозволів	Сторонні конектори, безпека на рівні документів, зіставлення ролей
Пошук на веб-сайтах	Надання відповідних та актуальних результатів	Веб-сканування, інкрементне індексування, кешування запитів
Пошук обслуговування клієнтів	Знаходження релевантних рішень, керування доступом, відстежування показників	Граф знань, доступ на основі ролей, аналітика
Чат-боти та RAG	Увімкнення можливості спілкування, надайння контексту, підтримка знань	Векторний пошук, моделі машинного навчання, інтеграція з базами знань
Географічний пошук	Обробка запитів про місцезнаходження, сортування за близькістю, фільтрація за площею текстом для отримання гібридних результатів	Геомапування, просторова індексація, обчислення дистанцій

Elasticsearch складається з таких компонентів (рисунок 2.3.) [27]:

Кластер. Кластер може складатися з одного або багатьох вузлів. Операції пошуку та індексації об’єднані між усіма вузлами кластера. Він ідентифікується унікальним ім’ям.

Вузол. Вузол є окремим сервером у кластері. Він ідентифікується унікальним ім'ям. Унікальне ім'я важливе тоді, коли існує намір встановити кілька вузлів в одній системі.

Індекс. Індекс представлений в Elasticsearch як колекція документів.

Документ. Документ являє собою базову одиницю вимірювання інформації, яка виражається у форматі JSON.

Шард. Фрагмент індексу, який дозволяє розподіляти дані по різних вузлах кластера. Кожен шард є окремим індексом Lucene, що лежить в основі роботи Elasticsearch. Це дозволяє розподіляти операції індексації й пошуку між кількома система одночасно для одного користувача або потоку.

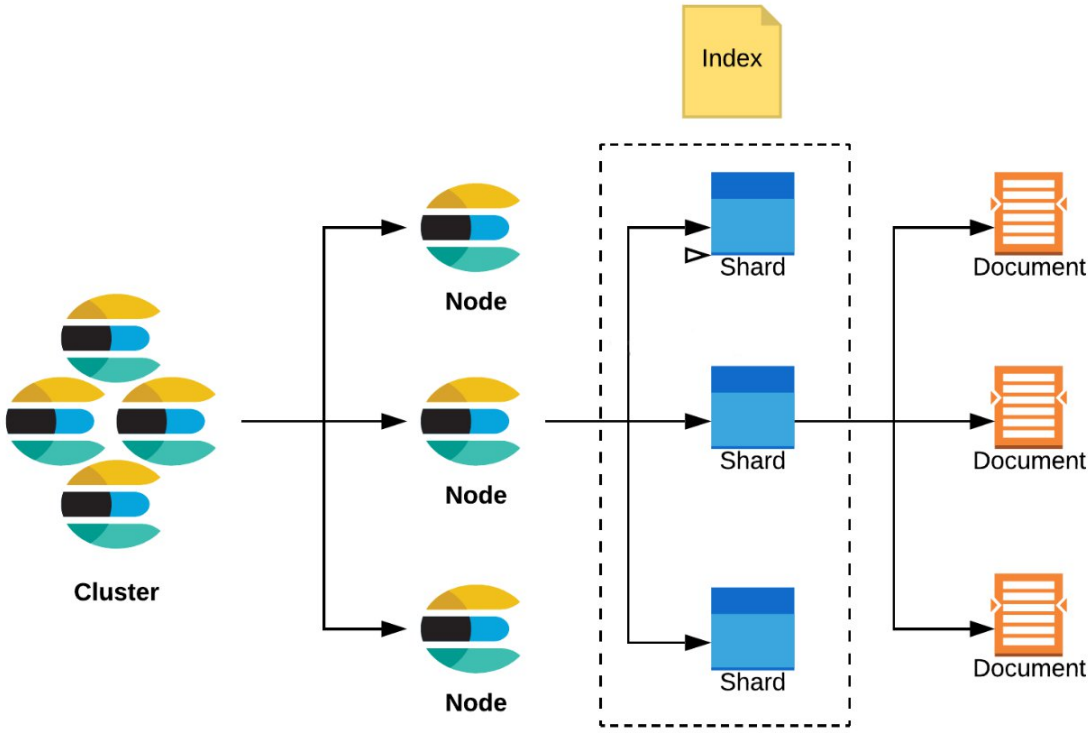

Рис. 2.3. Компоненти Elasticsearch [27]

MinIO – високопродуктивна розподілена система об'єктного зберігання з відкритим кодом, створена для приватних і гібридних хмар. Завдяки простій архітектурі вона забезпечує масштабованість, швидкість і надійність. Підходить як для резервного копіювання та архівування, так і для задач машинного навчання та аналітики.

Розроблена для роботи в хмарі і може працювати як легкий контейнер, керований зовнішніми службами управління, такими як Kubernetes. Весь сервер являє собою статичний двійковий файл і ефективно використовує ресурси процесора і пам’яті, де можна розмістити велику кількість користувачів на спільному обладнанні.

MinIO працює на стандартних серверах з локально підключеними дисками. Всі сервери в кластері рівні за можливостями і немають окремих вузлів імен чи серверів метаданих. Дані та метадані зберігаються разом як єдині об’єкти, усуваючи необхідність у базі метаданих. Крім того, усі ключові функції (код стирання, перевірка цілісності даних, шифрування) виконуються вбудовано та послідовно для відмовостійкості MinIO.

MinIO реалізована для великомасштабних хмарних сховищ даних з декількома центрами обробки даних. Кожен користувач використовує власний кластер MinIO, повністю ізольований від інших користувачів, що дозволяє захистити його від будь-яких перебоїв у роботі під час модернізації, оновлень або інцидентів безпеки [28].

На рис. 2.4. показано структуру сховища даних MinIO [28].

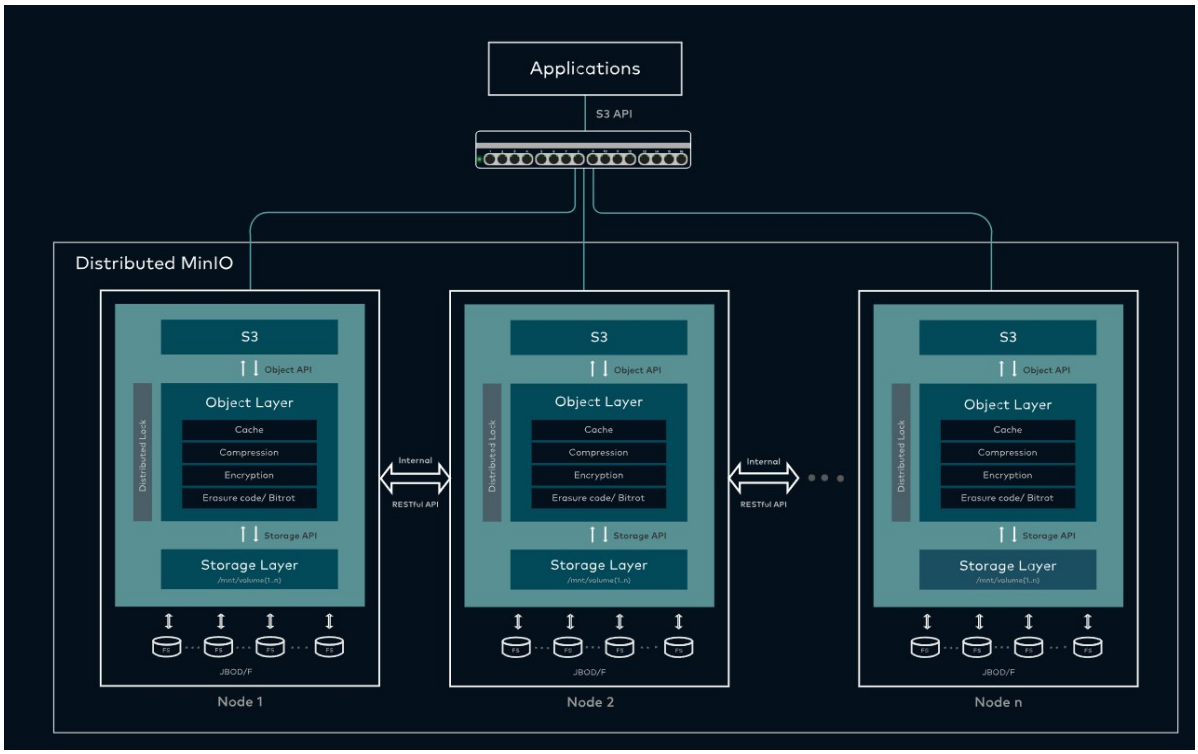

Рис. 2.4. Структура сховища даних MinIO [28]

Особливості MinIO включають у себе [28]:

Кодування зі стиранням (Erasure Coding). MinIO захищає дані за допомогою вбудованого кодування стирання на основі коду Ріда-Соломона, написаного на асемблері для максимальної продуктивності. Об'єкти розбиваються на блоки даних і парності з налаштовуваною надмірністю. Кодування забезпечує відновлення на рівні об'єктів – кожен об'єкт може відновлюватися окремо. При максимальній парності N/2 система здатна працювати з лише ((N/2) + 1) активними дисками. У конфігурації з 12 дисками MinIO розбиває об'єкти на 6 дисків даних і 6 дисків парності і може надійно записувати нові об'єкти або реконструювати існуючі об'єкти, використовуючи лише 7 дисків, що залишилися в розгортанні.

Захист від бітрот (Bitrot Protection). Бітрот (Bitrot) становить серйозну проблему дискових накопичувачів, що призводить до непомітного псування даних. Причинами можуть бути зношення дисків, стрибки напруги, помилки прошивки чи драйверів тощо. Цілісність забезпечується від початку до кінця шляхом обчислення хешу на READ і перевірки його на WRITE з програми, через мережу, пам'ять або на накопичувач.

Шифрування (Encryption). MinIO забезпечує повноцінний захист даних як під час передачі, так і в стані спокою. Він підтримує серверне та клієнтське шифрування, гарантує конфіденційність, цілісність і автентичність з мінімальним впливом на продуктивність. Дані шифруються автоматично на рівні об'єктів і захищаються за допомогою систем управління ключами.

Управління ідентифікацією (Identity Management). MinIO підтримує сучасні стандарти управління ідентифікацією, інтегруючись з провайдерами OpenID. Спрощує управління користувачами та забезпечує безпеку в багатокористувацьких і багатоекземплярних розгортань.

Безперервна реплікація (Continuous Replication). Безперервна реплікація MinIO розроблена для масштабованої синхронізації даних між дата-центрами, хмарами та регіонами. Завдяки подієвій моделі з використанням метаданих і лямбда-сповіщень, реплікація виконується миттєво й ефективно, без потреби у пакетній обробці. Вона мінімізує втрати даних навіть за умов високої динаміки. Крім того, реплікація є му-

льтивендорною, тобто резервні копії можуть зберігатися в будь-якому сумісному сховищі.

Глобальна федерація (Global Federation). MinIO підтримує глобальну федерацію, дозволяючи об'єднувати кілька розподілених екземплярів у єдиний простір імен із централізованим адмініструванням. Забезпечує масштабованість для великих, географічно розподілених підприємств і дає змогу керувати даними та додатками з однієї консолі.

Мультихмарний шлюз (Multi-Cloud Gateway). MinIO забезпечує уніфікований доступ до даних у приватних і публічних хмарах, перетворюючи різнорідну інфраструктуру на єдиний об'єктний шар, сумісний з Amazon S3 API. Це дозволяє додаткам працювати з даними однаково, незалежно від їхнього розташування, без потреби в міграції. Завдяки цьому організації можуть реалізувати справжню мультихмарну стратегію та уніфікувати зберігання даних.

Загалом, компоненти TheHive 5 утворюють гнучку та масштабовану архітектуру, яка забезпечує ефективне зберігання, обробку та пошук даних для підтримки процесів реагування на інциденти безпеки.

2.3. Процеси функціонування рішення TheHive 5

Для забезпечення безперервної роботи і продуктивності рішення TheHive 5 існують процеси функціонування, які охоплюють керування основними компонентами системи [29]:

операції кластера Cassandra;

операції безпеки Cassandra;

операції кластера MinIO;

операції резервного копіювання та відновлення (Backup and Restore).

Операції кластера Cassandra

Для забезпечення надійної роботи кластера Apache Cassandra у межах платформи TheHive 5 необхідно виконувати низку операцій, спрямованих на масштабу-

вання, обслуговування та підвищення відмовостійкості системи. До них належать [29]:

Додавання нового вузла до кластера (Adding a Node). Для масштабування Cassandra дозволяє додавати нові вузли, які автоматично приєднуються до кільця кластеру після налаштування відповідної конфігурації *cassandra.yaml* і запуску процесу *bootstrap*. Після додавання вузла проводиться балансування даних, що дозволяє оптимізувати навантаження.

Видалення активного вузла з кластера Cassandra (Removing an Alive Node). У випадках, коли вузол більше не потрібен, його можна безпечно вивести з експлуатації за допомогою команди nodetool decommission. Це забезпечує автоматичне переміщення реплік даних на інші активні вузли.

Видалення непрацюючого вузла з кластера Cassandra (Removing a Dead Node). Якщо вузол вийшов з ладу і не підлягає відновленню, його видалення здійснюється через команду nodetool removenode. Перед цим потрібно переконатися, що вузол дійсно недоступний за допомогою nodetool status, та замінити <*node_id*> на ідентифікатор непрацюючого вузла.

Збільшення коефіцієнта реплікації (Increasing Replication Factor). Для підвищення доступності та надійності даних у Cassandra можна змінити фактор реплікації (replication factor) через оновлення стратегії реплікації в *keyspace*. Після цього необхідно вручну запустити процес nodetool repair, щоб забезпечити синхронізацію даних згідно з новими параметрами.

Операції безпеки Cassandra

Для захисту даних у кластері Apache Cassandra реалізовані ключові механізми безпеки, що забезпечують аутентифікацію користувачів та шифрування каналів зв’язку [30]:

Аутентифікація в Cassandra (Authentication with Cassandra). Для контролю доступу до кластера застосовується механізм аутентифікації користувачів. Cassandra перевіряє облікові дані користувача при підключенні, забезпечуючи, що лише авторизовані користувачі мають доступ до даних і ресурсів кластера.

Шифрування зв'язку між вузлами (Node-to-Node Encryption). Для забезпечення безпеки комунікації між окремими вузлами кластера використовується шифрування трафіку. Це запобігає можливості перехоплення або модифікації даних під час їхнього обміну між серверами Cassandra.

Шифрування зв'язку клієнт-вузол (Client-to-Node Encryption). Для захисту даних, які передаються між клієнтськими додатками та вузлами кластера, застосовується шифрування каналів зв'язку, яке забезпечує конфіденційність і цілісність інформації при її передачі мережею.

Операції кластера MinIO

Для ефективного управління кластером MinIO у платформі TheHive 5 важливо слід виконувати наступні операції [31]:

Заміна диска (Replace a Disk). Якщо один із дисків у кластері вийшов з ладу або потребує заміни, його можна безпечно замінити без зупинки роботи кластера. MinIO автоматично відновить дані на новому диску, забезпечуючи цілісність і доступність інформації.

Заміна вузла (Replace a Node). У разі необхідності заміни апаратного або програмного вузла, MinIO дозволяє вивести старий вузол з кластера та додати новий, зберігаючи при цьому стан і конфігурацію, що надасть безперервність роботи без втрати даних.

Додавання вузла до кластера (Add a Node to the Cluster). Для масштабування сховища можна додати нові вузли до існуючого кластера. Після додавання вузол інтегрується в кластер, і система автоматично розподіляє дані, покращуючи продуктивність та розширюючи обсяг зберігання.

Видалення вузла з кластера (Remove a Node from Cluster). Під час видалення вузла з кластера MinIO потрібно дотримуватися тієї ж процедури, що й під час додавання вузла, а саме оновити файл конфігурації кластера, щоб відобразити видалення, та перезапустити усі вузли в кластері, щоб застосувати зміни.

MinIO і висока доступність (MinIO and High Availability). MinIO підтримує високу доступність, налаштовуючи одну кінцеву точку S3 в додатках, таких як TheHive 5. Для досягнення високої доступності між вузлами MinIO рекомендується

використовувати балансувальники навантаження та віртуальні IP-адреси для рівномірного розподілу з’єднань між вузлами кластера.

Операції резервного копіювання та відновлення (Backup and Restore)

Операції резервного копіювання та відновлення забезпечують збереження та відновлення даних у разі збоїв або необхідності перенесення системи. Існують два основні підходи [32]:

Холодне резервне копіювання та відновлення (Cold Backup & Restore). Холодне резервне копіювання передбачає повну зупинку всіх сервісів TheHive перед початком процесу, що гарантує цілісність даних, оскільки під час копіювання не відбуваються зміни в базі даних чи індексах.

Гаряче резервне копіювання та відновлення. Гаряче резервне копіювання дозволяє створювати резервні копії без зупинки сервісів, що особливо важливо для систем з високими вимогами до доступності. Однак цей підхід вимагає ретельного планування та врахування специфіки компонентів системи.

Належне функціонування TheHive 5 ґрунтується на правильно організованих процесах управління кластерами, дотриманні вимог безпеки та ефективному резервному копіюванні. Сукупність цих дій забезпечує безперервність роботи системи, її стійкість до збоїв та готовність до масштабування відповідно до потреб організації.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ БЕЗПЕКИ В КІНЦЕВИХ ТОЧКАХ ОРГАНІЗАЦІЇ НА БАЗІ THEHIVE 5

3.1. Порядок виявлення та реагування на інциденти безпеки в кінцевих точках організації на базі TheHive 5

У цьому розділі буде описано порядок виявлення та реагування на інциденти в кінцевих точках організації з використанням рішення TheHive 5.

Інтеграція TheHive 5 із Wazuh

Щоб TheHive 5 зміг отримувати сповіщення (Alerts), слід здійснювати наступні кроки інтеграції з ситемою моніторингу Wazuh за документацією [33]:

Спочатку в TheHive 5 потрібно створити нову організацію (Organisation) у веб-інтерфейсі TheHive з обліковим записом адміністратора (див. рис. 3.1.).

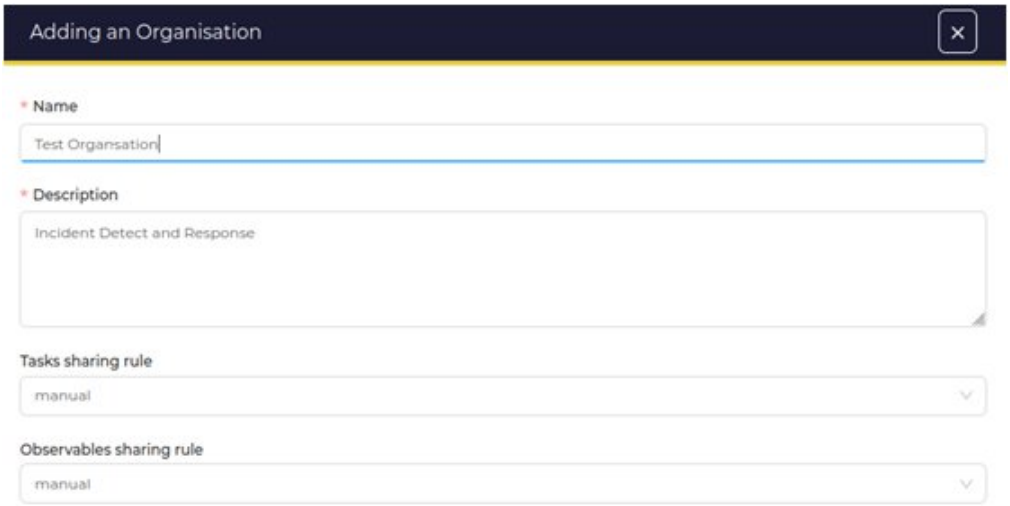

Рис. 3.1. Створення нової організації

Організації (Organizations) є клієнтами та користувачами, які діють як клієнти або користувачі та самостійно працюють з TheHive 5. Вони працюють незалежно одна від одної, з власними користувачами, кейсами та алертами. За потреби організації можна зв’язати між собою для обміну даними. Один користувач може

бути учасником кількох організацій, маючи різні ролі в кожній. Кількість активних організацій обмежується типом ліцензії. [34].

Далі у тестовій організації створюємо нового користувача з правами адміністратора організації (див. рис. 3.2.).

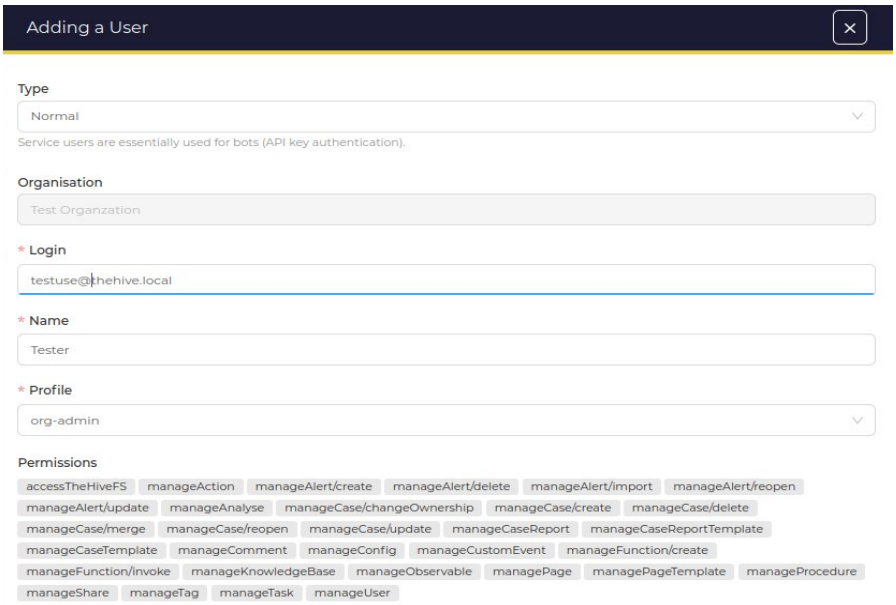

Рис. 3.2. Створення нового користувача з правами доступу

У TheHive 5 існує два типи облікових записів користувачів [35]:

Звичайні облікові записи. Призначені для доступу через веб-інтерфейс. Вони підтримують усі методи автентифікації та можуть генерувати API-ключі, якщо їх увімкнено..

Сервісні облікові записи. Створені для програмного доступу через API. Вони автентифікуються виключно за допомогою API-ключа та не мають доступу до веб-інтерфейсу.

Інтеграція з Wazuh можлива за допомогою REST API у TheHive 5. Тому потрібно перейти до щойно створеного користувача та згенерувати API Key (див. рис. 3.3.).

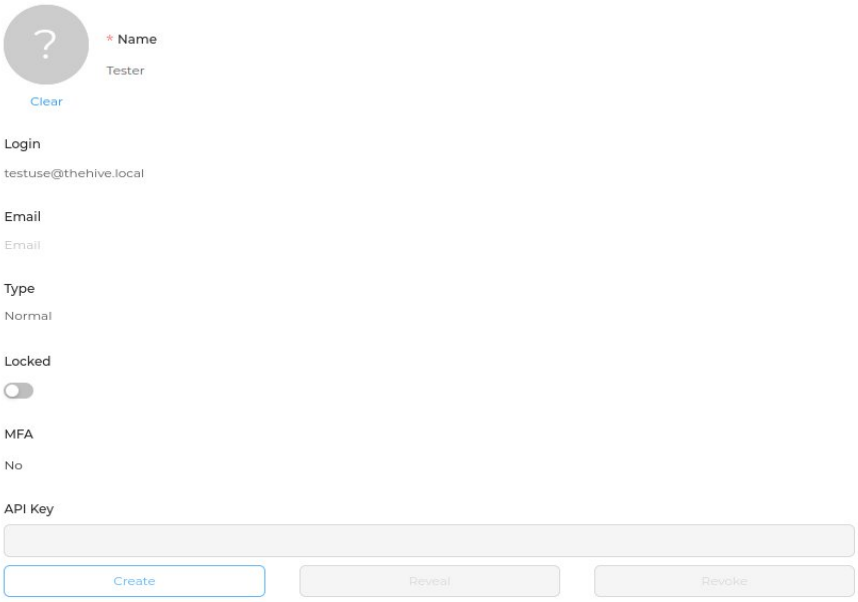

Рис. 3.3. Генерації API Key для Інтеграція з Wazuh

Далі будуть здійснюватися дії, щодо налаштування менеджера Wazuh. Перш за все, слід встановити модуль TheHive Python (див. рис. 3.4.).

```
hive5@hive5-VirtualBox:~$ sudo /var/ossec/framework/python/bin/pip3 install thehive4py==1.8.1
[sudo] password for hive5:
Collecting thehive4py==1.8.1
  Downloading thehive4py-1.8.1-py3-none-any.whl.metadata (4.3 kB)
Requirement already satisfied: future in /var/ossec/framework/python/lib/python3.10/site-packages (from thehive4py==1.8.1) (0.18.3)
```

Рис. 3.4. Встановлення модуля TheHive Python

Наступним кроком буде встановити скрипт інтеграції, вставляючи код Python у файл */var/ossec/integrations/custom-w2thive.py*. Змінна *lvl_threshold* вказує мінімальний рівень сповіщень, який буде пересилатися до TheHive (див. рис. 3.5.).

```
#!/var/ossec/framework/python/bin/python3
import json
import sys
import os
import re
import logging
import uuid
from thehive4py.api import TheHiveApi
from thehive4py.models import Alert, AlertArtifact
#start user config
# Global vars
#threshold for wazuh rules level
lvl_threshold=0
#threshold for suricata rules level
suricata_lvl_threshold=3
debug_enabled = False
#info about created alert
info_enabled = True
#end user config
# Set paths
pwd = os.path.dirname(os.path.dirname(os.path.realpath(__file__)))
log_file = '{0}/logs/integrations.log'.format(pwd)
logger = logging.getLogger(__name__)
```

Рис. 3.4. Скрипт інтеграції

Після цього створюємо *bash script* як */var/ossec/integrations/custom-w2thive*, який виконуватиме *.py script* (див. рис. 3.6.).

```
#!/bin/sh
# Copyright (C) 2015-2020, Wazuh Inc.
# Created by Wazuh, Inc. <info@wazuh.com>.
# This program is free software; you can redistribute it and/or modify it under the terms of GP>
WPYTHON_BIN="framework/python/bin/python3"
SCRIPT_PATH_NAME="$0"
DIR_NAME="$(cd $(dirname ${SCRIPT_PATH_NAME}); pwd -P)"
SCRIPT_NAME="$(basename ${SCRIPT_PATH_NAME})"
case ${DIR_NAME} in
    */active-response/bin | */wodles*)
        if [ -z "${WAZUH_PATH}" ]; then
            WAZUH_PATH="$(cd ${DIR_NAME}/../..; pwd)"
        fi
    PYTHON_SCRIPT="${DIR_NAME}/${SCRIPT_NAME}.py"
    ;;
    */bin)
    if [ -z "${WAZUH_PATH}" ]; then
        WAZUH_PATH="$(cd ${DIR_NAME}/..; pwd)"
    fi
    PYTHON_SCRIPT="${WAZUH_PATH}/framework/scripts/${SCRIPT_NAME}.py"
    ;;
     */integrations)
        if [ -z "${WAZUH_PATH}" ]; then
            WAZUH_PATH="$(cd ${DIR_NAME}/..; pwd)"
        fi
    PYTHON_SCRIPT="${DIR_NAME}/${SCRIPT_NAME}.py"
    ;;
esac
${WAZUH_PATH}/${WPYTHON_BIN} ${PYTHON_SCRIPT} $@
```

Рис. 3.6. Створення *bash script*

Щоб Wazuh міг запустити скрипт інтеграції, треба додати рядки до файлу конфігурації менеджера, розташованого за адресою */var/ossec/etc/ossec.conf*. У цьому скрипті потрібно вставити IP-адресу сервера TheHive разом із ключем API (див. рис. 3.7.).

```
<ossec_config>
  <global>
    <jsonout_output>yes</jsonout_output>
    <alerts_log>yes</alerts_log>
    <logall>no</logall>
    <logall_json>no</logall_json>
    <email_notification>no</email_notification>
    <smtp_server>smtp.example.wazuh.com</smtp_server>
    <email_from>wazuh@example.wazuh.com</email_from>
    <email_to>recipient@example.wazuh.com</email_to>
    <email_maxperhour>12</email_maxperhour>
    <email_log_source>alerts.log</email_log_source>
    <agents_disconnection_time>10m</agents_disconnection_time>
    <agents_disconnection_alert_time>0</agents_disconnection_alert_time>
    <update_check>yes</update_check>
  </global>

  <alerts>
    <log_alert_level>3</log_alert_level>
    <email_alert_level>12</email_alert_level>
  </alerts>

  <integration>
    <name>custom-w2thive</name>
    <hook_url>http://127.0.0.1:9000</hook_url>
    <api_key></api_key>
    <alert_format>json</alert_format>
  </integration>
```

Рис. 3.7. Додані рядки для запуску інтеграції

На завершення треба ввести команди для перезавантаження *wazuh-manager* та перевірки його працездатність (див. рис. 3.8. та рис. 3.9.).

```
hive5@hive5-VirtualBox:~$ sudo /var/ossec/bin/wazuh-control restart
2025/06/03 21:25:09 wazuh-modulesd:router: INFO: Loaded router module.
2025/06/03 21:25:09 wazuh-modulesd:content_manager: INFO: Loaded content_manager module.
wazuh-clusterd not running...
```

Рис. 3.8. Перезавантаження wazuh-manager

```
hive5@hive5-VirtualBox:~$ sudo systemctl status wazuh-manager
[sudo] password for hive5:
● wazuh-manager.service - Wazuh manager
     Loaded: loaded (/lib/systemd/system/wazuh-manager.service; enabled; vendor preset: enabled)
     Active: active (exited) since Tue 2025-06-03 21:24:16 EEST; 11h ago
      Tasks: 0 (limit: 27337)
     Memory: 0B
     CGroup: /system.slice/wazuh-manager.service

чер 03 21:24:08 hive5-VirtualBox env[111981]: Started wazuh-analysisd...
чер 03 21:24:09 hive5-VirtualBox env[111981]: Started wazuh-syscheckd...
чер 03 21:24:10 hive5-VirtualBox env[111981]: Started wazuh-remoted...
чер 03 21:24:11 hive5-VirtualBox env[111981]: Started wazuh-logcollector...
чер 03 21:24:13 hive5-VirtualBox env[111981]: Started wazuh-monitord...
чер 03 21:24:13 hive5-VirtualBox env[112357]: 2025/06/03 21:24:13 wazuh-modulesd:router: INFO: Loaded router module.
чер 03 21:24:13 hive5-VirtualBox env[112357]: 2025/06/03 21:24:13 wazuh-modulesd:content_manager: INFO: Loaded content_manager module.
чер 03 21:24:14 hive5-VirtualBox env[111981]: Started wazuh-modulesd...
чер 03 21:24:16 hive5-VirtualBox env[111981]: Completed.
чер 03 21:24:16 hive5-VirtualBox systemd[1]: Started Wazuh manager.
```

Рис. 3.9. Перевірка роботи wazuh-manager

Тест на виявлення інцидентів безпеки

Здійснемо декілька підозрілих дій у системі, щоб потім побачити нові сповіщення в TheHive 5 на вкладці «Alerts» (див. Рис. 3.10.).

```
hive5@hive5-VirtualBox:~$ for i in {1..10}; do ssh -o StrictHostKeyChecking=no u
ser@localhost; done
ssh: connect to host localhost port 22: Connection refused
ssh: connect to host localhost port 22: Connection refused
ssh: connect to host localhost port 22: Connection refused
ssh: connect to host localhost port 22: Connection refused
ssh: connect to host localhost port 22: Connection refused
ssh: connect to host localhost port 22: Connection refused
ssh: connect to host localhost port 22: Connection refused
ssh: connect to host localhost port 22: Connection refused
ssh: connect to host localhost port 22: Connection refused
ssh: connect to host localhost port 22: Connection refused
hive5@hive5-VirtualBox:~$ powershell.exe -EncodedCommand aGVsbG8gd29ybGQ=
powershell.exe: command not found
hive5@hive5-VirtualBox:~$ sudo nano eicar.txt
[sudo] password for hive5:
hive5@hive5-VirtualBox:~$
```

Рис. 3.10. Здійснення підозрілих дій у системі

Після цього знову увійдемо в TheHive 5 на вкладку «Alerts» (див. рис. 3.11.).

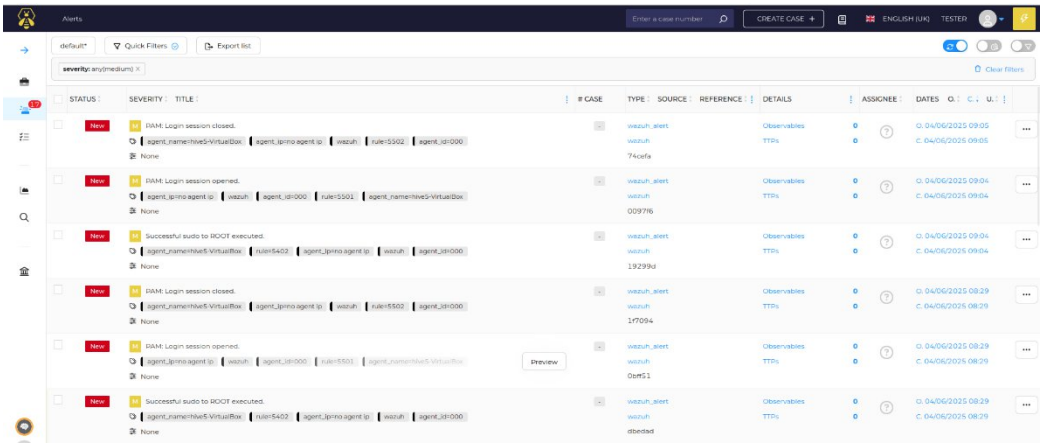

Рис. 3.11. Поява нових сповіщень

Сповіщення (Alerts) є подією безпеки, що генерується інструментами виявлення, брандмауери або платформи розвідки загроз. Воно служить раннім попередженням, яке допомагає аналітикам виявляти, досліджувати та реагувати на потенційні загрози.

Сповіщення розглядаються, сортуються і перетворюються на кейси (, якщо потрібне подальше розслідування. [36].

Аналіз інцидентів безпеки

Перед тим як здійснювати реагування, слід проаналізувати виявлений інцидент. Для цього потрібно вибрати подію і перейти до вкладки «General» (див. рис. 3.12.).

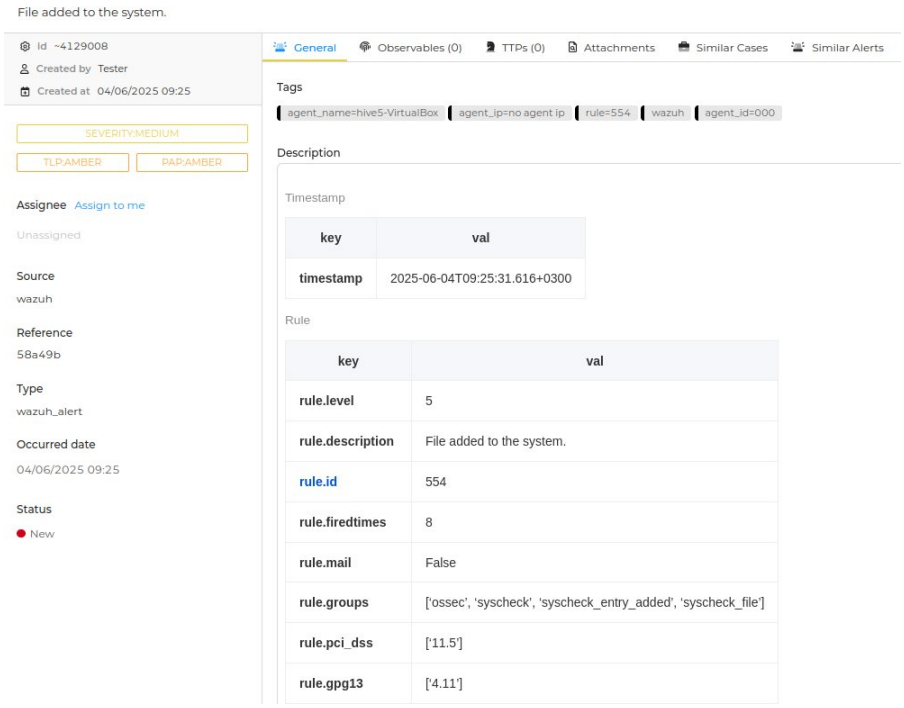

Рис. 3.12. Аналіз інциденту безпеки

Наприклад, подія File added to the system має такі параметри інциденту:

Severity – medium

TLP – amber

PAP – amber

Tags – agent_name=hive5-VirtualBox, rule=554, agent_id=000, wazuh, agent_ip=no agent ip

rule.level – 5

rule.id – 554

rule.firedtimes – 8

rule.mail – False

rule.groups – [‘ossec’, ‘syscheck’, ‘syscheck_entry_added’, ‘syscheck_file’]

full_log – File '/etc/systemd/system/multi-user.target.wants/snap-snapd-24505.mount' added

syscheck.path – /etc/systemd/system/multi-user.target.wants/snap-snapd-24505.mount

Створення кейсу для реагування на інциденти безпеки

Кейс (Case) являє структуровану сутність, яка використовується для відстеження, розслідування та реагування на інциденти безпеки, загрози або підозрілу діяльність. Вона служить центральним сховищем, де команди безпеки упорядковують інформацію, співпрацюють у розслідуваннях та документують свої висновки [37].

Щоб почати процес реагування на інциденти безпеки за допомогою кейсів, то слід перейти у верхній частині панелі TheHive 5 на вкладку «Create case». Там обрати «Empty Case» і призначити заголовок, дату виникнення події, рівень серйозності, TLP, PAP, теги та обис інциденту (див. рис. 3.13.).

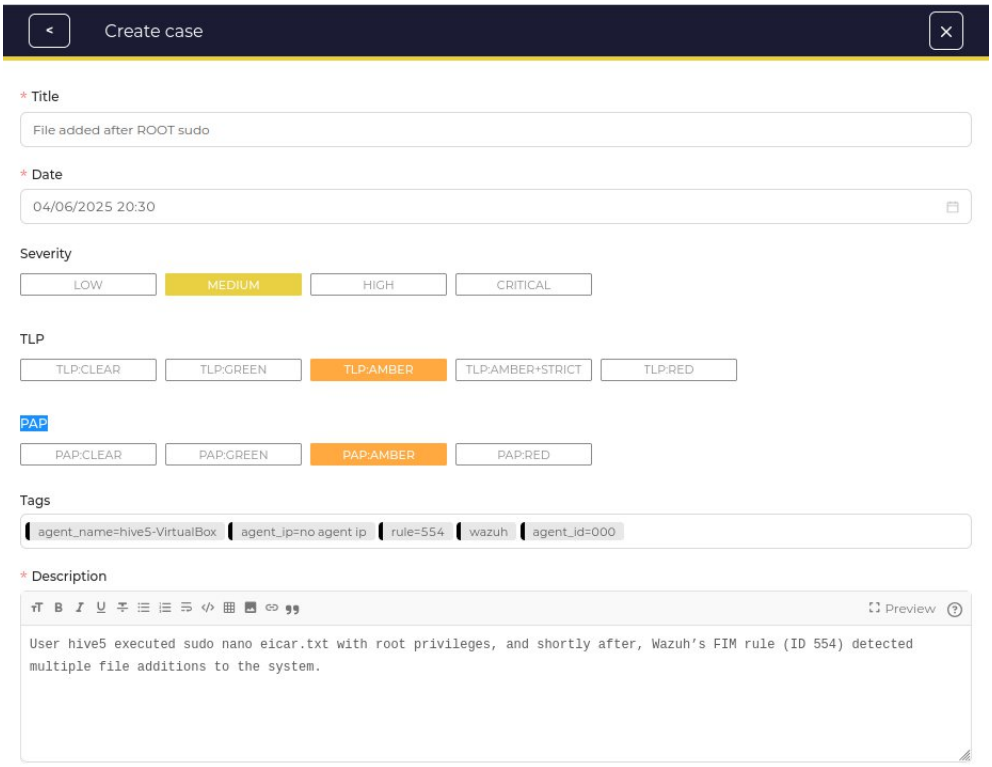

Рис. 3.13. Створення кейсу для реагування на інциденти безпеки

Створення завдань для управління кроками реагування

Завдання (Task) являє собою одну або декілька дій, які необхідно виконати в рамках кейсу. Вони можуть бути обов'язковими або необов'язковими, а також організовуються в групи для покращення структури та управління [38].

Для створення завдання потрібно перейти нижче у вікні «Create case» до «Tasks» та натиснути на «Add task». Тут прописуються групи завдань, заголовок завдання, опис необхідних дій, а також вибирається обов'язковість (mandatory), призначення (assignee) та позначення завдання (flag this task) (див. рис. 3.14.).

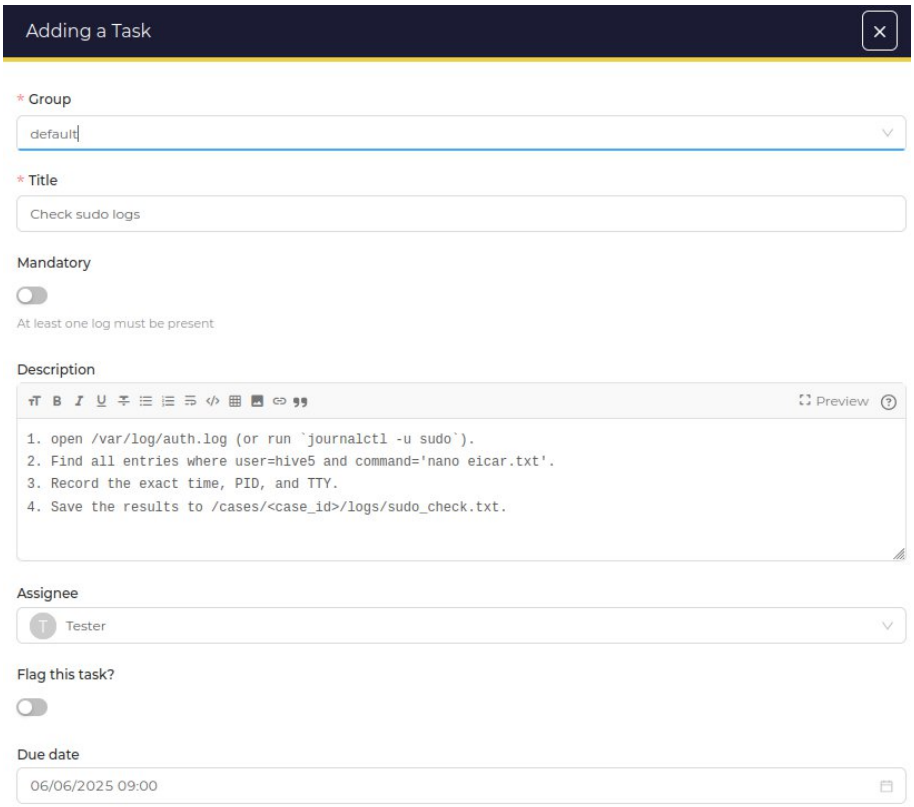

Рис. 3.14. Створення завдання для управління кроками реагування

Звітування про інцидент безпеки

Після того, як кейс був створений, додані туди всі завдання й іншу інформацію, можна експортувати результати у доволі зручному форматі для формування звітів. Щоб це зробити, потрібно обрати потрібний кейс та натиснути на «Export selection». У вікні запропонують формат екпорту даних у вигляді CSV або JSON.

Відкриваємо цей файл переглядаємо експортовану інформацію з кейсу (див. рис. 3.15.).

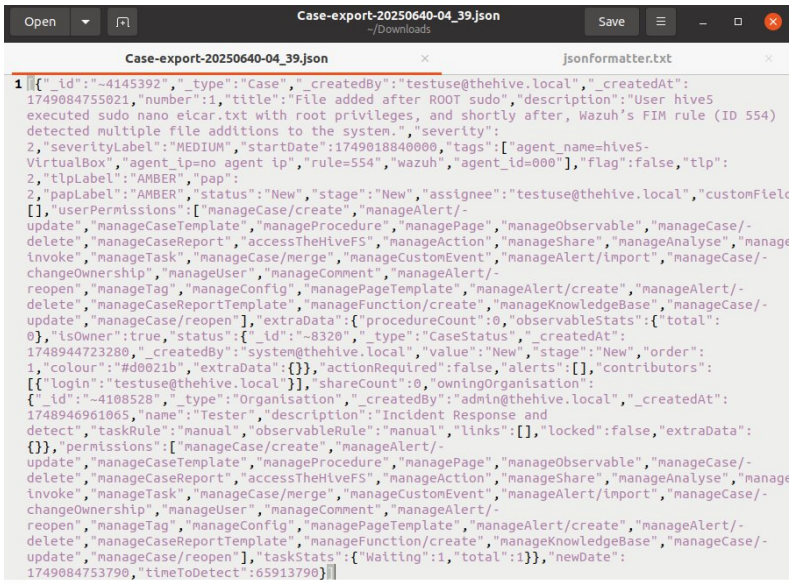

Рис. 3.15. Експорт даних з кейсу

Такий порядок виявлення та реагування на інциденти безпеки в кінцевих точках організації на базі рішення TheHive 5 дозволить фахівцям з кібербезпеки оперативно і скоординовано реагувати та виявляти загрози, зменшувати час на ідентифікацію інцидентів безпеки, а також покращувати ефективність аналізу, документування та подальшого вдосконалення заходів безпеки.

3.2. Рекомендації щодо виявлення та реагування на інциденти безпеки в кінцевих точках організації

Впровадьте регулярний моніторинг стану кінцевих точок

Організуйте систематичну перевірку:

Періодично контролюйте стан ресурсів, таких як CPU, пам'ять, мережеві підключення для виявлення аномалій;

Здійснюйте перевірку встановленого програмного забезпечення та запущених процесів для своєчасного виявлення незапланованих змін;

Запровадьте щоденний огляд базових логів операційної системи на предмет підозрілих подій.

Впровадьте централізовану систему збору логів подій

Забезпечте збір і зберігання системних та користувацьких подій з усіх кінцевих точок:

Уніфікуйте формат логів та зберігайте їх у захищеному сховищі.

Аналізуйте логи на предмет аномалій.

Організуйте централізований збір і аналіз повідомлень про помилки та збої

Вчасно виявляйте системні проблеми:

Запровадьте процедуру передачі повідомлень про критичні збої у відповідний відділ.

Аналізуйте повторювані помилки як потенційний симптом інциденту безпеки чи збою.

Використовуйте отримані дані для планування профілактичних заходів.

Організуйте навчання персоналу

Підвищуйте обізнаність співробітників щодо потенційних загроз та ознак інцидентів безпеки:

Проводьте тренінги з розпізнавання ознак зараження пристроїв;

Ознайомте працівників із базовими правилами безпечної роботи.

Використайте стандартні сценарії реагування (playbooks)

Дійте за затвердженим планом:

Дотримуйтеся покрокових інструкцій щодо перевірки, очищення та відновлення системи;

Не намагайтеся самостійно усунути проблему без відповідної кваліфікації;

Залучайте технічних фахівців для безпечного видалення шкідливих компонентів.

Повідомте відповідальні зовнішні організації

У разі серйозного інциденту дотримуйтесь законодавчих вимог:

Повідомте відповідну національну команду реагування (наприклад, CERT-UA).

Зберіть необхідні документи для аудиту чи внутрішнього розслідування.

Координуйте дії з партнерами, якщо інцидент торкнувся спільних систем.

Проведіть аналіз інциденту та оновіть процедури безпеки

Вивчіть інцидент і впровадьте заходи, щоб запобігти його повторенню в майбутньому:

Складіть звіт про інцидент безпеки;

Оновіть політики та навчальні матеріали.

Оформіть звіт про інцидент бещпеки

Фіксуйте всі деталі для архіву та звітності:

Опис події, дата, час, залучені особи, вжиті дії.

Висновки щодо причин, ризиків і вжитих змін.

Передайте звіт відповідальному відділу.

ВИСНОВКИ

У кваліфікаційній роботі було досліджено актуальність проблеми виявлення та реагування на інциденти безпеки в кінцевих точках організації. Аналіз показав, що в сучасному світі цифрових технологій обсяг інцидентів безпеки постійно зростає, що робить необхідним впровадження надійних і ефективних засобів виявлення та реагування. Інциденти безпеки можуть завдати значної шкоди як окремим користувачам, так і організаціям в цілому, спричиняючи втрату контролю над інформаційними ресурсами, викрадення конфіденційних даних та порушення нормального функціонування інформаційних систем, що може призвести до фінансових збитків і втрати довіри.

Розглядалися підходи до виявлення та реагування на інциденти безпеки в кінцевих точках організації, а саме основні заходи та етапи щодо виялення та реагування на інциденти безпеки в кінцевих точках.

У рамках роботи було здійснено детальний огляд існуючих рішень для виявлення та реагування на інциденти безпеки в кінцевих точках організації. Особливу увагу було приділено аналізу Velociraptor, InsightIDR та GRR Rapid Response. Було розглянуто призначення, особливості даних рішень, архітектуру та компоненти.

TheHive 5 було вивчено як дієву платформу, що забезпечує реагування на інциденти безпеки в кінцевих точках. Її сильними сторонами є тісна інтеграція з MISP та Cortex, підтримування співпраці в режимі реального часу, має гнучке управління завданнями та кейсами, сучасний інтерфейс користувача, покращене управління сповіщеннями та високу якість реагування на інциденти безпеки.

Практичне значення одержаних результатів полягає в тому, що порядок виявлення та реагування на інциденти безпеки в кінцевих точках може бути використаний організаціями для покращення своєї кібербезпеки.

На основі проведеного дослідження розроблено рекомендації фахівцям з кібербезпеки щодо виявлення та реагування на інциденти безпеки в кінцевих точках

організації. Запропоновані заходи дають змогу збільшити стійкість до інцидентів безпеки в кінцевих точках.

Таким чином, мета кваліфікаційної роботи досягнута, всі поставлені завдання виконано, а отримані результати мають як теоретичною, так і практичною цінністю.

ПЕРЕЛІК ПОСИЛАНЬ

1. 2024 Unit 42 Incident Response Report: Navigating the Shift in Cybersecurity Threat Tactics. Palo Alto Networks. URL: https://unit42.paloaltonetworks.com/unit42-incident-response-report-2024-threat-guide/ (дата звернення: 23.04.2025).

2. Кібератака на українську енергетику: як це було. URL: https://texty.org.ua/fragments/65835/Kiberataka_na_ukrajinsku_jenergetyku_jak_ce_bulo-65835/ (дата звернення: 24.04.2025).

3. Історія вірусу NotPetya: чи варто остерігатися подібних кібератак в майбутньому?. URL: https://www.imena.ua/blog/notpetya-cyberattack/ (дата звернення: 24.04.2025).

4. Scroxton A. Ukraine cyber teams responded to more than 2,000 attacks in 2022. URL: https://www.computerweekly.com/news/252529292/Ukraine-cyber-teams-responded-to-more-than-2000-attacks-in-2022 (дата звернення: 25.04.2025).

5. Коваль О. Якою була атака хакерів на «Київстар» та як відновлювалась компанія. URL: https://dou.ua/lenta/news/kyivstar-cyber-attack-restoration/ (дата звернення: 25.04.2025).

6. Оліщук І. До відключення опалення у Львові взимку 2024 року причетні російські хакери. URL: https://zaxid.net/do_vidklyuchennya_opalennya__u_lvovi_vzimku_2024_roku_prichetni_rosiyski_hakeri_n1590134 (дата звернення: 25.04.2025).

7. Нафтогаз заявляє про кібератаку.URL: https://www.ukrinform.ua/rubric-economy/3818060-naftogaz-zaavlae-pro-kiberataku.html (дата звернення: 26.04.2025).

8. The NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP. 29 February 26, 2024. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (дата звернення

02.05.2025).

9. Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-61 Revision 2. Paul R. Cichonski, Thomas Millar, Timothy Grance, Karen Scarfone URL: https://www.nist.gov/publications/computer-security-incident-handling-guide (дата звернення 03.05.2025).

10. Patel A. Exploring Velociraptor: A Versatile Tool for Incident Response and Digital Forensics. URL: https://www.cyberengage.org/post/exploring-velociraptor-a-versatile-tool-for-incident-response-and-digital-forensics (дата звернення 05.05.2025).

11. Deployment Overview | Velociraptor documentation. Velociraptor. URL: https://docs.velociraptor.app/docs/deployment/ (дата звернення 05.05.2025).

12. InsightIDR Overview - Getting Started with InsightIDR | InsightIDR documentation. InsightIDR. URL https://docs.rapid7.com/insightidr/insightidr-overview (дата звернення 07.05.2025).

13. Collector Overview - Setup and Deployment | InsightIDR documentation. InsightIDR. URL: https://docs.rapid7.com/insightidr/collector-overview (дата звернення 07.05.2025).

14. Insight Agents with InsightIDR - Setup and Deployment | InsightIDR documentation. InsightIDR. URL: https://docs.rapid7.com/insightidr/insight-agent (дата звернення 07.05.2025).

15. Insight Network Sensor Overview - Event Source Configuration | InsightIDR documentation. InsightIDR. URL: https://docs.rapid7.com/insightidr/insight-network-sensor-overview (дата звернення 07.05.2025).

16. Cloud Services - Event Source Configuration | InsightIDR documentation. InsightIDR. URL: https://docs.rapid7.com/insightidr/cloud-service/ (дата звернення 08.05.2025).

17. Insight Orchestrator overview - Setup and Deploy an Orchestrator | InsightIDR documentation. InsightIDR. URL: https://docs.rapid7.com/insightcon-

nect/orchestrator/ (дата звернення 08.05.2025).

18. What is GRR? | GRR documentation. GRR. URL: https://grr-doc.readthedocs.io/en/latest/what-is-grr.html (дата звернення 11.05.2025).

19. Overview - Installing and Running GRR | GRR documentation. GRR. URL: https://grr-doc.readthedocs.io/en/latest/installing-and-running-grr/overview.html (дата звернення 11.05.2025).

20. Overview | TheHive 5 documentation. TheHive 5. URL: https://docs.strangebee.com/thehive/overview/ (дата звернення 13.05.2025).

21. TheHive 5.0 is now available. TheHive 5. URL: https://strangebee.com/blog/thehive-5-0-is-now-available/ (дата звернення 13.05.2025).

22. TheHive v5.1: New features. TheHive 5. URL: https://strangebee.com/blog/thehive-5-1-new-features/ (дата звернення 14.05.2025).

23. Overview - Architecture | Cassandra documentation. Apache Cassandra. URL: https://cassandra.apache.org/doc/latest/cassandra/architecture/overview.html (дата звернення 16.05.2025).

24. Apache Cassandra Architecture Definition. Apache Cassandra.URL: https://www.scylladb.com/glossary/apache-cassandra-architecture/ (дата звернення 16.05.2025).

25. Elasticsearch basics - Elasticsearch Guide | Elastic documentation. Elasticsearch. URL: https://www.elastic.co/guide/en/elasticsearch/reference/8.18/elasticsearch-intro-what-is-es.html#elasticsearch-intro-use-cases (дата звернення 18.05.2025).

26. Solutions and use cases | Elastic documentation. Elasticsearch. URL: https://www.elastic.co/docs/solutions/search (дата звернення 18.05.2025).

27. Sam C. Different Elasticsearch components and what they mean in 5 mins. URL: https://devopsideas.com/different-elasticsearch-components-and-what-they-mean-in-5-mins/ (дата звернення 19.05.2025).

28. Product Overview. MinIO. URL: https://min.io/product/overview (дата звернення 19.05.2025).

29. Cassandra Cluster Operations - Operations. TheHive 5 documentation. The-

Hive 5. URL: https://docs.strangebee.com/thehive/operations/cassandra-cluster/ (дата звернення 21.05.2025).

30. Security in Apache Cassandra - Operations. TheHive 5 documentation. TheHive 5. URL: https://docs.strangebee.com/thehive/operations/cassandra-security/ (дата звернення 21.05.2025).

31. MinIO Cluster Operations - Operations |TheHive 5 documentation. The-Hive 5. URL: https://docs.strangebee.com/thehive/operations/minio-cluster/ (дата звернення 21.05.2025).

32. Overview - Backup & Restore Operations - Operations | TheHive 5 documentation. TheHive 5. URL: https://docs.strangebee.com/thehive/operations/backup-restore/overview/ (дата звернення 21.05.2025).

33. Ishiaku A. Using Wazuh and TheHive for threat protection and incident response. Wazuh. URL: https://wazuh.com/blog/using-wazuh-and-thehive-for-threat-protection-and-incident-response/ (дата звернення 26.05.2025).

34. About Organizations - Organizations - Administration Guides | TheHive 5 documentation. TheHive 5. URL: https://docs.strangebee.com/thehive/administration/organizations/about-organizations/ (дата звернення 28.05.2025).

35. User Accounts - Organization Administration - User Guides | TheHive 5 documentation. TheHive 5. URL: https://docs.strangebee.com/thehive/user-guides/organization/configure-organization/manage-user-accounts/about-user-accounts/ (дата звернення 28.05.2025).

36. Alerts Management - Analyst’s Corner - User Guides | TheHive 5 documentation. TheHive 5. URL: https://docs.strangebee.com/thehive/user-guides/analyst-corner/alerts/about-alerts/ (дата звернення 28.05.2025).

37. Cases Management - Analyst’s Corner - User Guides | TheHive 5 documentation. TheHive 5. URL: https://docs.strangebee.com/thehive/user-guides/analyst-corner/cases/about-cases/#case-visibility (дата звернення 29.05.2025).

38. Tasks Management - Analyst’s Corner - User Guides | TheHive 5 documentation. TheHive 5. URL: https://docs.strangebee.com/thehive/user-guides/analyst-

corner/tasks/about-tasks/ (дата звернення 29.05.2025).