МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Сумський державний університет
Центр заочної, дистанційної та вечірньої форм навчання
Кафедра комп'ютерних наук

«До захисту допущено»
В.о. завідувача кафедри
Ігор ШЕЛЕХОВ
(підпис)
11 грудня 2023 р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня магістр

зі спеціальності 122 - Комп'ютерних наук,
освітньо-професійної програми «Інформатика»
на тему: «Інформаційна технологія забезпечення корпоративної кібербезпеки»
здобувачки групи ІН.мз-21с Козачок Юлії Олександрівни

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

Юлія КОЗАЧОК
(підпис)

Керівник,
завідувач кафедри кібербезпеки,
к.ф.-м.н., професор Володимир ЛЮБЧАК
(підпис)

Суми – 2023

Сумський державний університет
Центр заочної, дистанційної та вечірньої форм навчання
Кафедра комп'ютерних наук

«Затверджую»
В.о. завідувача кафедри
_____ Ігор ШЕЛЕХОВ
(підпис)

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня магістра

зі спеціальності 122 - Комп'ютерних наук, освітньо-професійної програми «Інформатика»
здобувачки групи ІН.мз-21с Козачок Юлії Олександрівни

1. Тема роботи: «Інформаційна технологія забезпечення корпоративної кібербезпеки» затверджую наказом по СумДУ від *«20» листопада 2023 р. № 1308-VI*
2. Термін здачі здобувачем кваліфікаційної роботи *до 13 грудня 2023 року*
3. Вхідні дані до кваліфікаційної роботи _____
4. Зміст розрахунково-пояснювальної записки (перелік питань, що їх належить розробити) *1) Аналіз проблеми предметної області, постановка й формування завдань дослідження. 2) Огляд технологій та рішень функціонування SOC. 3) Розробка рішень по підвищенню ефективності SOC. 4) Аналіз результатів.*
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)_____
6. Консультанти до проекту (роботи), із значенням розділів проекту, що стосується їх

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв

7. Дата видачі завдання «____» _____ 20 ___ р.

Завдання прийняв до виконання _____ (підпис) Керівник _____ (підпис)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапів кваліфікаційної роботи	Термін виконання	Примітка
1	*Аналіз проблеми предметної області, постановка й формування завдань дослідження*	14.10.2023	Виконано
2	*Огляд технологій та рішень функціонування SOC*	25.10.2023	Виконано
3	*Розробка рішень по підвищенню ефективності SOC*	15.11.2023	Виконано
4	*Аналіз отриманих результатів*	22.11.2023	Виконано
5	*Оформлення пояснювальної записки до кваліфікаційної роботи*	01.12.2023	Виконано

Здобувачка вищої освіти _____ (підпис) Керівник _____ (підпис)

АНОТАЦІЯ

Записка: 69 стор., 44 рис., 1 додаток, 20 використаних джерел.

Обґрунтування актуальності теми роботи – тема кваліфікаційної роботи є актуальною, оскільки присвячена розв'язанню важливої практичної задачі підвищення ефективності SOC шляхом розробки відповідних рішень.

Об'єкт дослідження — центр управління інформаційною безпекою організації.

Мета роботи — оцінка ефективності інформаційних технологій та управлінських рішень забезпечення діяльності SOC на прикладі обраної організації та розробка рекомендацій щодо її підвищення.

Методи дослідження — оцінка поточних процесів та інструментів SOC, аналіз інцидентів, аудит персоналу та технологій, а також розробка рекомендацій для підвищення ефективності SOC через використання відповідних методологій.

Результати — у результаті роботи проведено аналітичний огляд основних принципів функціонування SOC та його інформаційних технологій, розглянуто питання організації людських та технічних ресурсів. Також визначено критерії оцінки ефективності SOC, проведено її вимірювання. Виконано розробку кількох інструментів для покращення ефективності SOC і проведено практичну реалізацію цих рішень. За результатами виконаної роботи підготовлені рекомендації по підвищенню ефективності функціонування SOC.

SECURITY OPERATIONS CENTER, SIEM,
SOAR, КОРПОРАТИВНА КІБЕРБЕЗПЕКА.

ЗМІСТ

ПЕРЕЛІК ТЕРМІНІВ ТА СКОРОЧЕНЬ

IT, information technologies, інформаційні технології	–	Інтеграція методів, виробничих процесів і програмно-технічних засобів, які використовуються для збирання, опрацювання, зберігання, розповсюдження, показу і використання інформації в інтересах її користувачів.
IT-система	–	Сукупність програмних і апаратних засобів, а також організаційне забезпечення, які надають інформаційну підтримку в наданні послуг Компанією.
Monitoring system, система моніторингу	–	Система, що здійснює контроль за роботою обладнання, встановленого на мережі Замовника.
Playbook, файл сценаріїв	–	Рекомендовані дії для кожного типу порушень (у тому числі й перелік ситуацій, коли необхідно здійснити відключення сервісів, щоб уникнути витоку або порушення цілісності інформації, що є найбільш критичним для всієї діяльності Замовника).
SIEM, Security information and event management, система управління інформацією про безпеку та події безпеки	–	Програмно–апаратний комплекс, призначений для виявлення Інцидентів, збору і зберігання лог–файлів пристроїв і додатків з метою їх подальшого аналізу, кореляції і нормалізації.

SLA, Service Level Agreement, Угода про рівень послуг	–	Офіційне зобов'язання між Постачальником послуг і Замовником з узгодженням рівня якості, наявності та відповідальності. Показник, що відображає рівень відпрацювання Інцидентів у SIEM згідно з чисельними та якісними метриками надання інформації про події на мережі Замовника в залежності від послуг, що надаються.
SOAR, Security Orchestration, Automation and Response, оркестрація подій безпеки і автоматичного реагування	–	Набір функцій технології: оркестрація для інтеграції із засобами захисту та іншими IT-системами підприємства, автоматизація за рахунок заздалегідь описаних кроків розслідування (Playbook) виявлених інцидентів і реагування на них за допомогою оркестрації.
TI, threat intelligence, кіберрозвідка	–	Діяльність, спрямована на збір відомостей і вивчення даних про противника з метою аналізу і прогнозування його дій, а також інших цілей, що стоять перед командою розвідників. Це дані про появу нових шкідливих програм, націлених на бізнес Замовника і на його клієнтів, а також про витік, продажі баз даних, пошук інсайдерів в Компанії і обговореннях уразливості її систем.
Агент	–	Комплекс програм та продуктів, що розгортається чи встановлюється на

		операційну систему Замовника, дозволяє здійснювати збір даних з джерела подій і надає інформацію в SIEM.
АС, автоматизована система	–	Технологія, яка дозволяє персоналу виконувати встановлені функції за допомогою засобів автоматизації.
БД, база даних	–	Сукупність даних, які пов'язані між собою певним чином і підтримують одну або кілька областей застосування.
Джерело даних	–	Набір елементів ПЗ і обладнання Замовника та агентів SOC (кінцевий пристрій або система), що підтримує хронологію і здатний бути комплексним джерелом достовірної інформації для фіксації зміни контрольованих параметрів, оперативного аналізу та прийняття рішень.
Довідник Інцидентів	–	Перелік основних можливих Інцидентів і ознак порушень (проникнень).
Додаток	–	Складова частина документу, що уточнює, роз’яснює, доповнює його зміст або набуває чинності на підставі основного документа. Додатки мають документи всіх видів – й організаційно-розпорядчі, й інформаційно-аналітичні.
Етап реагування	–	Перелік дій за певний проміжок часу з реагування на Інцидент та його локалізації,

		починаючи від реєстрації оператором в SIEM. Залежить від рівня критичності Інциденту.
Журнал подій	–	Компонент, який дозволяє переглядати лог подій на локальному комп'ютері або на віддаленій машині, включаючи доступ, видалення, додавання файлу або програми, зміну дати системи, завершення роботи системи, зміна конфігурації системи і т. д.
Замовник	–	Юридична особа, яка замовляє певні роботи чи послуги з надання інформаційної безпеки в ОД, подає заявку на замовлення таких послуг у майбутньому та в подальшому обслуговується ОД.
ЗЗІ, засоби захисту інформації	–	Сукупність програмних та апаратних засобів, призначених для захисту інформації від несанкціонованого доступу, використання, модифікації, знищення або розголошення.
ІБ, інформаційна безпека	–	Стан, при якому інформація захищена від несанкціонованого доступу, використання, модифікації та знищення.
Інцидент	–	Зміна параметрів стану кінцевого пристрою або системи, що виникає в результаті збою чи іншого порушення роботи ІТ систем Замовника, перевищує задані граничні показники, і призводить або може призвести до відмови в наданні внутрішніх ІТ-послуг, або неприпустимого зниження рівня якості ІТ-

		послуги, чи виникнення загрози, у результаті якої велика ймовірність компрометації бізнес-процесів і загрози ІБ для організації. (Підтверджена подія, що вказує на минулу, поточну або ймовірну загрозу).
Клієнт	–	Потенційний Замовник послуг ОД.
Кореляція даних	–	Порівняння параметрів даних про події інформаційної безпеки з їх заданими граничними показниками для виявлення Інцидентів інформаційної безпеки.
Моніторинг	–	Комплекс технічних, технологічних, організаційних та інших засобів, які забезпечують систематичний контроль (стеження) за станом та тенденціями мережі та процесів, що відбуваються.
Нормалізація даних	–	Перетворення і приведення даних до єдиного формату для спрощення подальшої обробки.
ОД, Октава Дефенс	–	Постачальник послуг, що надає керовані сервіси кібербезпеки Замовнику згідно Договору.
Патч/оновлення	–	Додатковий програмний засіб, який застосовується для виправлення виявлених дефектів в програмному забезпеченні або зміни його функціоналу.
ПЗ, програмне забезпечення	–	Сукупність комплексу комп'ютерних програм і даних, призначених для розв'язання певного

кола завдань, що зберігаються в цифровому вигляді.

Подія	–	Початкова зареєстрована зміна параметрів стану кінцевого пристрою або системи в логах SIEM, пов'язана з некоректним функціонуванням IT-послуги чи апаратним забезпеченням, що може призвести до виникнення Інциденту, і дані про яку вносяться в системний журнал пристрою або системи.
Правила кореляції	–	Набір логічних правил, що дозволяють здійснювати порівняння параметрів подій інформаційної безпеки, а також їх кількості та частоти з заданими показниками для виявлення Інцидентів інформаційної безпеки.
Пріоритет	–	Параметр, який використовується для розуміння відносної важливості Інциденту, присвоюється кожному зареєстрованому в SOC Інциденту на мережі і залежить від типу і наслідків робіт. Пріоритет ґрунтується на впливі та терміновості і використовується для визначення необхідного часу обробки та порядку ліквідації інцидентів. Він визначається співвідношенням впливу і терміновості, а також використовується для визначення часу, необхідного для обробки та порядку ліквідації інцидентів.

Програмно-технічний комплекс	–	Сукупність апаратних, апаратно-програмних та програмних засоби, які використовуються для надання електронних довірчих послуг і забезпечують виконання функцій, пов’язаних з їх наданням.
Процес	–	Сукупність взаємопов'язаних або взаємодіючих видів діяльності, яка перетворює входи на виходи і вимагає для цього певних ресурсів і керуючих впливів.
Сервіс	–	Послуги, які Виконавець надає Замовнику відповідно до Договору
Система автоматизації	–	Інформаційно об'єднана сукупність програмованих пристроїв автоматизованого та автоматичного контролю, регулювання та керування.
ТІС, технічна інфраструктура	–	Сукупність уніфікованих технологій, програмного забезпечення, комп'ютерних систем, які дозволяють користувачам створювати, одержувати доступ, зберігати, передавати та змінювати інформацію.

ВСТУП

Обґрунтування вибору теми роботи. Оцінка ефективності SOC дозволяє виявити сильні та слабкі сторони системи, визначити напрями її подальшого розвитку та вдосконалення. Результати оцінки можуть бути використані для ухвалення управлінських рішень, спрямованих на підвищення ефективності SOC.

Актуальність. В наш час, в умовах стрімкого розвитку інформаційних технологій, зростання кількості кіберзагроз та ускладнення їх характеру, зростає і роль центрів забезпечення та управління інформаційною безпекою (SOC). Його неефективність може призвести до негативних наслідків, таких як недооцінка загроз інформаційної безпеки та втрата репутації. З урахуванням сутності проблеми та її негативних наслідків можна зробити висновок, що підвищення ефективності SOC є актуальним завданням для будь-якої організації, яка здійснює свою діяльність в умовах кіберзагроз.

Об’єкт дослідження. Центр управління інформаційною безпекою організації.

Предмет дослідження. Інформаційні технології та управлінські рішення підвищення ефективності SOC.

Гіпотеза. Ефективність SOC може бути підвищена шляхом аналізу поточних процесів та технологій, виявлення прогалин та розробки стратегій для їхнього усунення, що сприятиме покращенню виявлення та відповіді на кіберзагрози.

Наукова новизна. Унікальність полягає в поєднанні різних методик оцінки ефективності SOC, таких як аналіз інцидентів, аудит процесів та технологій, оцінка персоналу та використання підходів для отримання комплексного уявлення про стан центру безпеки.

Структура. Дана робота складається зі вступу, аналітичного огляду, постановки задачі, вибору методу розв’язання поставленої задачі, опису програмного забезпечення, висновків, списку використаних джерел та додатку.

РОЗДІЛ 1 – АНАЛІТИЧНИЙ ОГЛЯД ТЕХНОЛОГІЙ ТА РІШЕНЬ ФУНКЦІОНУВАННЯ SOC

1.1 Поняття та функції SOC

Операційний центр безпеки (SOC) – це централізована функція в організації, яка використовує людей, процеси та технології для постійного моніторингу та покращення стану безпеки організації (та її клієнтів), одночасно запобігаючи, виявляючи, аналізуючи та реагуючи на інциденти кібербезпеки [1].

Мережі, сервери, комп’ютери, кінцеві пристрої, операційні системи, програми та бази даних постійно перевіряються на наявність ознак інцидентів кібербезпеки. Команда SOC аналізує логи, встановлює правила та контролі, визначає винятки, покращує відповіді на інциденти та стежить за новими вразливими місцями.

З огляду на те, що технологічні системи в сучасній організації працюють 24/7, SOC зазвичай працюють цілодобово позмінно, щоб забезпечити швидке реагування на будь-які нові загрози. Команди SOC можуть співпрацювати з іншими відділами та співробітниками або працювати з експертами сторонніх постачальників IT-безпеки [2].

Члени команди SOC беруть на себе наступні функції, щоб допомагати запобігати атакам, реагувати та відновлюватися після атак:

1. Інвентаризація активів та інструментів

Щоб усунути сліпі плями та прогалини в охопленні, SOC потребує видимості активів, які він захищає, та розуміння інструментів, які він використовує для захисту організації. Це означає облік усіх баз даних, хмарних служб, ідентифікаторів, програм і кінцевих точок. Команда також відстежує всі рішення безпеки, які використовуються в організації, такі як брандмауери, програмне забезпечення для захисту від зловмисних програм, програм-вимагачів і ПЗ для моніторингу.

2. Зменшення поверхні атаки

Ключовим обов’язком SOC є зменшення поверхні атаки організації. SOC робить це, проводячи інвентаризацію всіх робочих активів, виявляючи неправильні конфігурації та додаючи нові активи, коли вони надходять в мережу. Члени команди також відповідають за дослідження загроз, що виникають, і їх аналіз, що допомагає їм бути в курсі останніх подій.

3. Безперервний моніторинг

Використовуючи рішення для аналітики безпеки, такі як рішення для корпоративного керування інформацією про безпеку (SIEM), рішення для автоматизації та реагування (SOAR) або рішення для розширеного виявлення та реагування (XDR), команди SOC контролюють усе середовище – локально, хмари, програми, мережі та пристрої – цілий день, щодня, щоб виявити аномалії чи підозрілу поведінку. Ці інструменти збирають телеметрію, агрегують дані та в деяких випадках автоматизують реагування на інциденти.

4. Розвідка загроз

SOC також використовує аналітику даних, зовнішні канали та звіти про загрози продукту, щоб отримати уявлення про поведінку зловмисників, інфраструктуру та мотиви. Цей процес надає широке уявлення про те, що відбувається в Інтернеті, і допомагає командам зрозуміти, як працюють групи зловмисників. Маючи цю інформацію, SOC може швидко виявити загрози та захистити організацію від нових ризиків.

5. Виявлення загроз

Команди SOC використовують дані, згенеровані рішеннями SIEM і XDR, для виявлення загроз. Це починається з фільтрації помилкових спрацьовувань від справжніх проблем. Потім вони впорядковують загрози за серйозністю та потенційним впливом на бізнес.

6. Керування журналами

SOC також відповідає за збір, підтримку та аналіз даних журналів, створених кожною кінцевою точкою, операційною системою, віртуальною машиною, локальною програмою та мережевою подією. Аналіз допомагає

встановити базову лінію для нормальної діяльності та виявляє аномалії, які можуть свідчити про зловмисне програмне забезпечення, програми-вимагачі або віруси.

7. Реагування на інцидент

Після виявлення кібератаки SOC швидко вживає заходів, щоб обмежити збитки для організації з якомога меншими порушеннями для бізнесу. Кроки можуть включати вимикання або ізоляцію уражених кінцевих точок і програм, призупинення скомпрометованих облікових записів, видалення заражених файлів і запуск антивірусного програмного забезпечення та програмного забезпечення для захисту від шкідливих програм.

8. Відновлення та санація

Після атаки SOC відповідає за відновлення початкового стану компанії. Команда зітре та повторно підключить диски, ідентифікаційні дані, електронну пошту та кінцеві точки, перезапустить програми, переключиться на системи резервного копіювання та відновить дані.

9. Дослідження першопричини

Щоб запобігти повторенню подібної атаки, SOC проводить ретельне розслідування, щоб виявити вразливості та недосконалі процеси безпеки, які сприяли інциденту.

10. Покращення безпеки

SOC використовує будь-які розвідувальні дані, зібрані під час інциденту, для усунення вразливостей, покращення процесів і політик і оновлення плану безпеки [3].

1.2 Організація людського ресурсу

Одна з перших складових кожного SOC – це люди. Загалом головні ролі в команді SOC включають:

- Менеджер SOC, який керує командою, наглядає за всіма операціями безпеки та звітує перед CISO організації (головним спеціалістом з інформаційної безпеки).

- Інженери, які створюють і керують архітектурою безпеки організації. Значна частина цієї роботи включає оцінку, тестування, рекомендації, впровадження та підтримку засобів і технологій безпеки. Інженери з безпеки також співпрацюють із командами розробників або DevOps/DevSecOps, щоб переконатися, що архітектура безпеки організації включає цикли розробки програм.
- Аналітики, які, по суті, першими реагують на загрози або інциденти кібербезпеки. Аналітики виявляють, досліджують і сортують (визначають пріоритети) загрози; потім вони ідентифікують постраждалі хости, кінцеві точки та користувачів і вживають відповідних заходів для пом'якшення та стримування впливу. У деяких організаціях слідчі та спеціалісти з реагування на інциденти є окремими ролями, класифікованими як аналітики рівня L1 та рівня L2 відповідно.
- «Мисливці» за загрозами (їх також називають експертами-аналітиками безпеки) спеціалізуються на виявленні та стримуванні розширених загроз – нових загроз або варіантів загроз, яким вдається прослизнути повз автоматичний захист [4].

На рисунку нижче (Рис. 1.1) наведена загальна організаційна структура SOC.

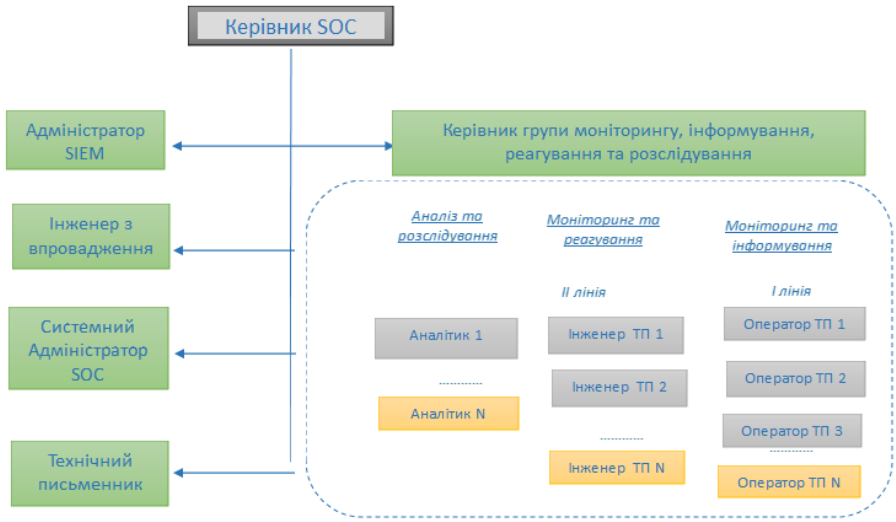


Рисунок 1.1 – Загальна організаційна структура SOC

Технічний відділ SOC «Октава Дефенс» складається з 2-х Адміністраторів SIEM, 2-х Інженерів, 3-х Аналітиків L2 та 5-ти Аналітиків L1. Детальний опис ролей, напрямів їх відповідальності та ключових особливостей в процесі керування Інцидентами на прикладі обраної організації описані нижче (Табл. 1.1).

Таблиця 1.1 – Ролі в процесі управління Інцидентами

Роль в процесі	**Належність**	**Функції в межах бізнес–процесу**
Оператор (Аналітик L1)	SOC	-Моніторинг подій та Інцидентів, що фіксує SIEM. -Проведення попередньої діагностики Інциденту згідно пріоритету та повноважень. -Усунення Інцидентів у разі відповідності зоні повноважень. -Внесення даних в SIEM при обробці Інциденту. -Ескалація запиту на Аналітика L2, якщо вирішення питання лежить поза зоною відповідальності. -Надання рекомендації для навчання SIEM.
Інженер	SOC	-Консультування Експертів Замовника щодо налаштування Автоматизованих систем. -Внесення/корегування даних в SIEM у разі змін в автоматизованих системах Замовника у відповідності з офіційним повідомленням тощо. -Реєстрація та надсилання відповідного запиту, якщо вирішення питання лежить в зоні відповідальності інших підрозділів чи Замовника. -Моніторинг вирішення питання іншими підрозділами та надання відповіді Замовнику. -Ескалація звернення чи Інциденту у випадку не отримання відповіді у встановлені терміни.
Аналітик L2	SOC	-Розслідування нетипових Інцидентів та робота з контентом SIEM. -Побудова процесів, корегування існуючих та налаштування нових інструментів на платформі аналізу SIEM та зовнішнього навчання.

		-Збір, узагальнення, аналіз інформації, прогнозування та надання консультацій із захисту мережі. -Прийняття та впровадження ефективних рішень для захисту інформації. -Підготовка звітів.
Адміністратор SIEM	SOC	-Встановлення, адміністрування, налаштування й конфігурування оновлень SIEM та ПЗ. -Встановлення, адміністрування, налаштування й конфігурування апаратного та програмного забезпечення. -Обслуговування та проектування мережі для повноцінного функціонування SIEM. -Моніторинг доступності SIEM. -Ведення IT–документації.

1.3 Інструменти SOC та технологічна модель

Загальну схему інструментів SOC та їх взаємодії на прикладі ОД можна побачити нижче (Рис. 1.2).

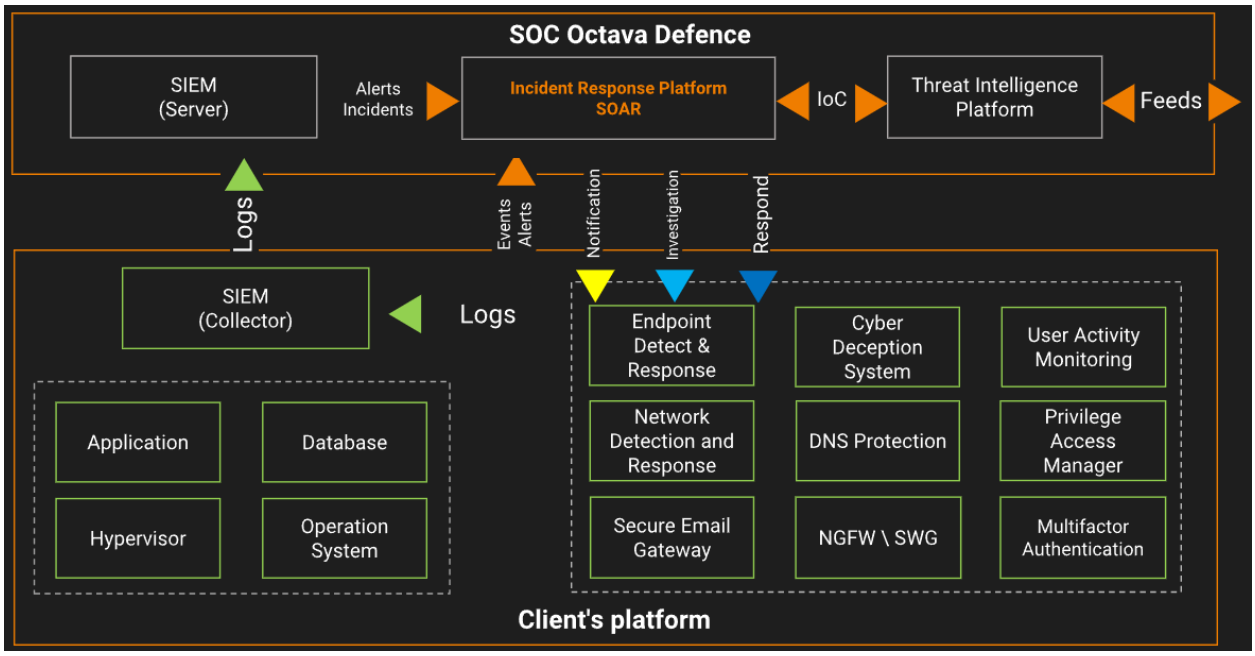


Рисунок 1.2 – Інструменти SOC та їх взаємодія

В якості платформи реагування на інциденти використовується рішення FortiSOAR. Воно має такі особливості і переваги:

— Комплексне рішення (500+ інтеграцій, 800 плейбуків, надійні функції, рішення для конкретних випадків підтримують ефективність SOC/NOC/OT);

— Модуль рекомендацій на основі ШІ (вбудований ШІ забезпечує автоматизацію та прийняття рішень, включаючи групування алертів, оцінювання загроз, плейбуки);

— Вбудована кіберрозвідка (вбудований інтелект FortiGuard Labs і публічних джерел збагачують розслідування);

— Контент-хаб та коммьюніті (коннектори, плейбуки, пакети рішень, відео з передовими практиками та спільнота);

— Створення плейбуків без коду/з кодом на мінімальному рівні (запатентований досвід дизайну забезпечує легке візуальне перетягування та швидкі режими розробки для створення плейбуків);

— Гнучкі варіанти розгортання (вибір SaaS, локального, публічного хмарного хостингу або надійних партнерів MSSP) [5].

Інтерфейс платформи FortiSOAR можна побачити нижче (Рис. 1.3)

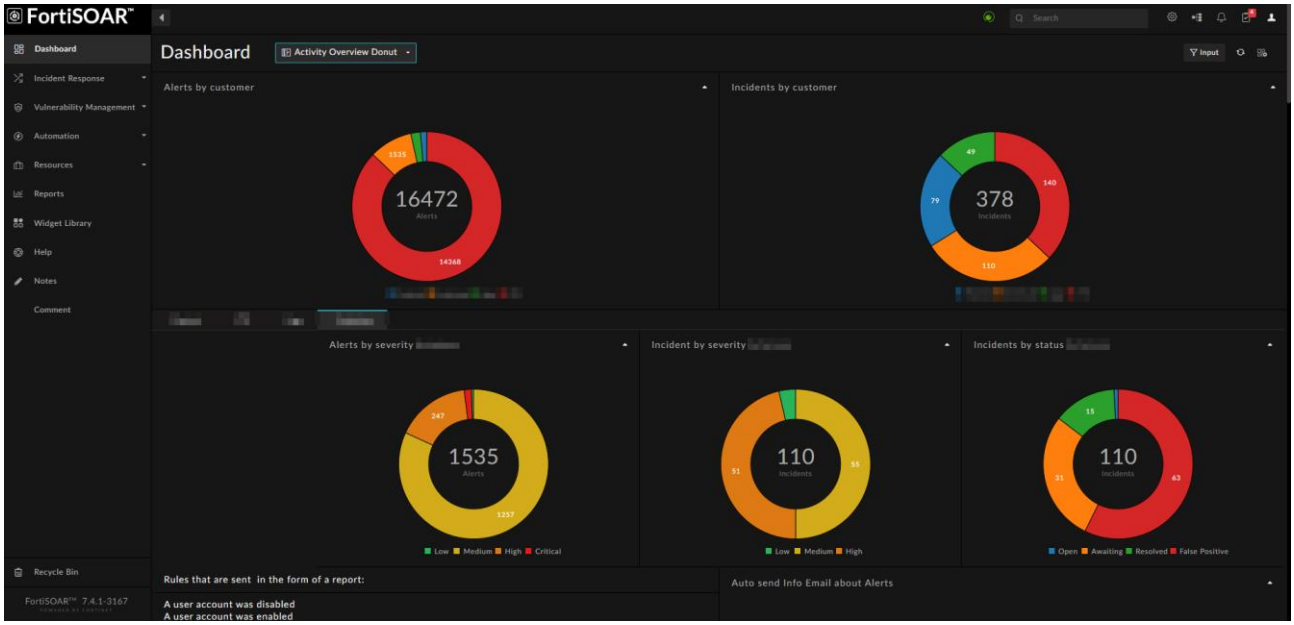


Рисунок 1.3 – Інтерфейс FortiSOAR

В якості SIEM-платформи використовується рішення від Elastic. Воно надає можливості для швидкого відстеження атак, що розгортаються, співвідносячи всі відповідні дані [6]. У своїй діяльності аналітики SOC ОД найчастіше використовують наступні вкладки:

1. Вкладка «Alerts» (Рис. 1.4) дозволяє обрати проміжок часу, що нас цікавить (1); відображає список правил, що спрацювали за цей час (2), а також надає інформацію про їхню природу та потенційні наслідки (3).

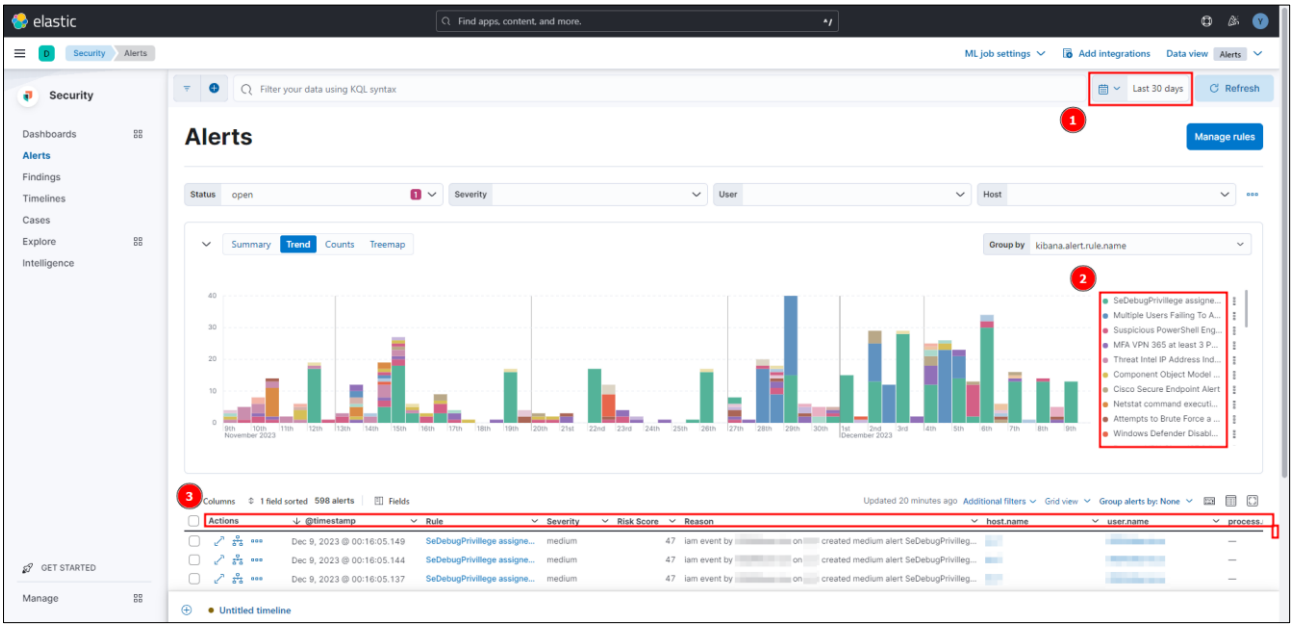


Рисунок 1.4 – Вкладка «Alerts»

2. Вкладка «Discover» (Рис. 1.5) дає більш детальну інформацію про всі логи, що надходять у систему (1).

Вона відповідає за пошук даних за ключовими словами, датами, значеннями та іншими параметрами (2); за фільтрування даних за різними критеріями та полями (такими як тип даних, джерело даних, дата та час, пов’язаний користувач і т.д.) (3); за візуалізацію даних за допомогою діаграм, графіків, карт.

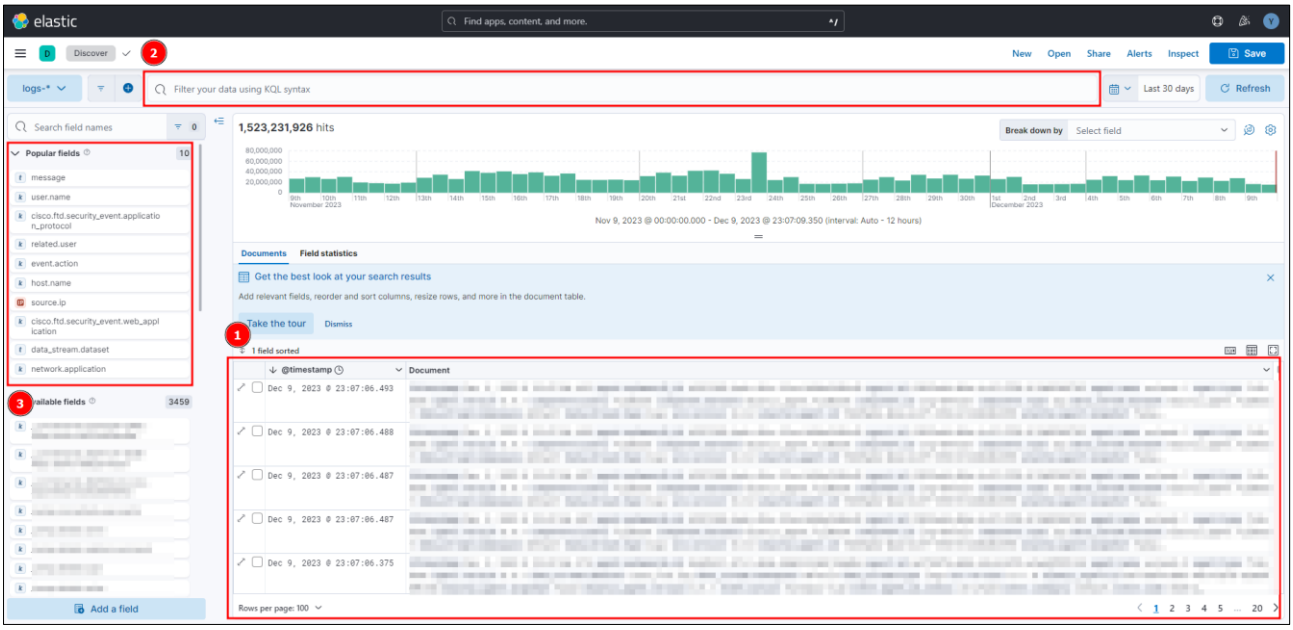


Рисунок 1.5 – Вкладка «Discover»

3. Вкладка «Dashboards» відповідає за створення та управління панелями керування. Панелі керування – це інтерактивні візуалізації даних, які дозволяють швидко та легко отримати доступ до потрібної інформації. Приклад одного з дашбордів можна побачити нижче (Рис. 1.6).

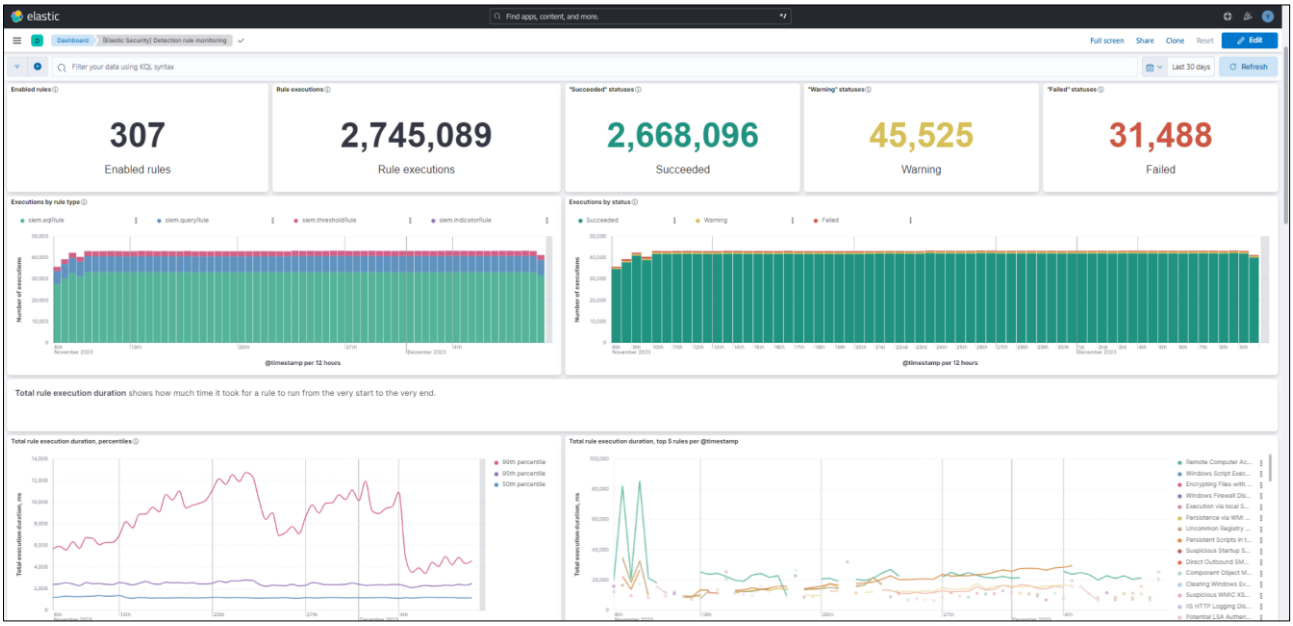


Рисунок 1.6 – Приклад дашборду

У Табл. 1.2 наведено список рішень, що співпрацюють з SIEM і використовуються для збору логів про активність в мережі Замовника.

Таблиця 1.2 – Рішення, що співпрацюють з SIEM

Назва рішення	**Опис**
Endpoint Detect & Response	Виявлення кінцевих точок і реагування на них, або EDR, – це програмне забезпечення, розроблене для автоматичного захисту кінцевих користувачів організації, кінцевих пристроїв і IT-активів від кіберзагроз, які оминають антивірусне програмне забезпечення та інші традиційні інструменти безпеки кінцевих точок [7]. EDR постійно збирає дані з усіх кінцевих точок мережі – настільних і портативних комп'ютерів, серверів, мобільних пристроїв, пристроїв IoT (Інтернет речей) тощо. Він аналізує ці дані в режимі реального часу на наявність доказів відомих або підозрюваних кіберзагроз і може автоматично реагувати, щоб запобігти або мінімізувати шкоду від виявлених загроз [8].
Network Detection & Response	Рішення для виявлення та реагування на мережу (NDR) використовують комбінацію розширених аналітичних методів, які не ґрунтуються на сигнатурах, як-от машинне навчання, щоб виявити підозрілу мережеву активність. Це дозволяє командам реагувати на аномальний або зловмисний трафік і загрози, які пропускають інші інструменти безпеки [9].
Secure Email Gateway	Захищений шлюз електронної пошти (SEG) або захищений сервер електронної пошти (SEC) – це тип ПЗ безпеки електронної пошти, який знаходиться між вхідною та вихідною електронною поштою [10]. Кожен електронний лист, який надсилається до та з організації, проходить через цей шлюз, щоб переконатися, що його вміст не є зловмисним або ознакою витоку даних. Він запобігає надходженню небажаних електронних листів у папки вхідних повідомлень користувачів, наприклад спаму, фішингових листів, електронних листів із шкідливим програмним забезпеченням тощо. У багатьох відношеннях шлюзи електронної пошти є першою лінією захисту електронної пошти [11].
Cyber Deception System	Це стратегія відволікання кіберзлочинців від справжніх активів підприємства та перенаправлення їх у приманку чи пастку. Приманка

	імітує законні сервери, програми та дані, щоб зловмисник був обманом змушений повірити, що він проник і отримав доступ до найважливіших активів підприємства, хоча насправді це не так. Стратегія використовується для мінімізації збитків і захисту справжніх активів організації [12].
DNS Protection	Ця система діє як щит, який захищає вашу мережу та системи від кіберзагроз, які використовують систему DNS. Вона контролює та відстежує вихідні DNS-запити, блокує шкідливі домени та захищає вашу мережу від шкідливих зловмисних програм або фішингових атак [13].
NGFW/SWG	Next Generation Firewall (міжмережевий екран наступного покоління) - відомий клас продуктів, що поєднує функціональність простих рішень на основі безпеки веб шлюзу (Secure Web Gateway, SWG) з класичними брандмауерами, антивірусами та IDS [14].
User Activity Monitoring	Моніторинг активності користувачів – це моніторинг і відстеження поведінки кінцевих користувачів на пристроях, мережах та інших IT-ресурсах компанії. Багато організацій впроваджують інструменти моніторингу активності користувачів, щоб допомогти виявити та зупинити внутрішні загрози, як ненавмисні, так і зі зловмисними намірами. Діапазон моніторингу та використовуваних методів залежить від цілей компанії [15]. Впроваджуючи моніторинг активності користувачів, підприємства можуть легше виявляти підозрілу поведінку та зменшувати ризики, перш ніж вони призведуть до витоку даних, або принаймні вчасно, щоб мінімізувати збитки. Моніторинг активності користувачів, який іноді називають відстеженням активності користувача, є формою стеження, але служить для проактивного перегляду активності кінцевого користувача, щоб визначити зловживання привілеями доступу або політикою захисту даних через незнання чи зловмисний намір [16].
Privilege Access Manager	Це рішення для захисту ідентичностей, яке дає змогу вбезпечити організацію від кіберзагроз, відстежуючи й виявляючи несанкціонований привілейований доступ до важливих ресурсів, а також запобігаючи йому [17]. Рішення PAM поєднує користувачів, процеси й технології, а також надає вичерпні відомості про те, хто і як

	використовує привілейовані облікові записи. Обмеження кількості користувачів із доступом до адміністративних функцій, допомагає посилити систему безпеки, а додаткові рівні захисту зменшують кількість випадків порушення безпеки даних [18].
Multifactor Authentication	Багатофакторна автентифікація – це процес входу в обліковий запис, який потребує кількох методів автентифікації з незалежних категорій облікових даних для перевірки особи користувача для входу чи іншої транзакції [19]. Багатофакторна автентифікація поєднує двоє або більше незалежних облікових даних – те, що знає користувач (наприклад пароль); те, що має користувач (наприклад маркер безпеки); і хто такий користувач, використовуючи методи біометричної перевірки [20].

РОЗДІЛ 2 – ПРИНЦИПИ, КРИТЕРІЇ ТА ПРОГРАМНІ ІНСТРУМЕНТИ ОЦІНКИ ЕФЕКТИВНОСТІ SOC

2.1 Фази керування інцидентами

Процес керування інцидентами можна поділити на декілька основних фаз. Основні етапи, напрямок керування, обов'язки з боку SOC та обов'язки з боку Замовника наведені в таблиці нижче (Табл. 2.1).

Таблиця 2.1 – Фази керування інцидентами

Фази керування інцидентами	**Напрямок**	**Обов'язки з боку SOC**	**Обов'язки з боку Замовника**
Підготовка	Побудова технічної інфраструктури, необхідної для роботи з інцидентами	-Обстеження інформаційної інфраструктури Замовника. -Розгортання програмно-апаратного комплексу.	-Надання логіки та топології мережі. -Визначення об'єктів моніторингу. --Організація передачі даних. -Організація захищеного каналу зв'язку.
	Створення правил виявлення інцидентів	Налаштування SIEM.	-Забезпечення даних, необхідних для налаштування SIEM – налаштування правил моніторингу та коригування кореляційних правил у SIEM.
Виявлення та аналіз інцидентів	Моніторинг і виявлення	Виконання функцій з моніторингу, аналізу та сповіщення Замовника.	-Надання Виконавцю списку контактних осіб для інформування.
	Аналіз інцидентів		
	Пріоритизація		
	Сповіщення		
Локалізація, нейтралізація та відновлення	Локалізація інциденту	Коригування стратегії локалізації.	-Визначення внутрішньої критичності, вибір стратегії локалізації.

			-Локалізація інцидентів.
	Нейтралізація	-Надання консультацій та рекомендацій щодо усунення та відновлення після інциденту. -Контроль виконання рекомендацій.	-Виконання робіт із усунення та відновлення після інциденту на інфраструктурі та бізнес додатках, активних засобах захисту. -Верифікація наданих консультацій.
	Відновлення після інциденту	Повна передача Замовнику.	Повністю виконується Замовником.
	Збір, зберігання та документування ознак інциденту	Залучення команди експертів/аналітиків для аналізу інциденту.	-Прийняття рекомендацій SOC для запобігання повторного виникнення. -Зберігання скомпрометованих систем.
	Розслідування інциденту	Надання рекомендацій Замовнику для запобігання повторного виникнення інцидентів.	Залучення команди експертів/аналітиків для аналізу причин виникнення інциденту.

2.1.1 Підготовка

Для фіксації та обробки інцидентів в інфраструктурі Замовника Виконавцю необхідно провести наступні дії:

- Обстеження Виконавцем інформаційної інфраструктури Замовника.

Фахівці Виконавця проводять обстеження (аудит) інформаційної інфраструктури Замовника. Замовник надає для аналізу архітектуру системи, її топології і складові елементи, типи користувачів системи, інформацію за типами, що обробляється в технічній інфраструктурі (ТІС).

За результатами виконання обстеження Виконавець отримує наступні документи:

— логіку та топологію ТІС (містить опис, принципи побудови і архітектуру);

— перелік об'єктів ТІС, що підлягають захисту і затверджуються Замовником.

- Розгортання програмно-.апаратного комплексу (сенсори) Виконавцем.

Варіанти розгортання:

— Комплекс може бути розгорнутий на апаратній або віртуальній платформі Замовника.

— Комплекс може бути розгорнутий на апаратній платформі Виконавця та розміщений в інфраструктурі Замовника.

Технічні характеристики програмно-апаратного комплексу визначаються в залежності від кількості та характеристик узгоджених продуктів та сенсорів згідно переліку об’єктів, що підлягають моніторингу. Вимоги до фізичного середовища, у якому буде розташований програмно-апаратний комплекс, визначаються після розрахунку технічних характеристик програмно-апаратного комплексу.

- Організація захищеного каналу зв’язку Замовником.

Для своєчасної та повної передачі даних від програмно-апаратного комплексу в інфраструктурі Замовника до місця розташування серверів керування та моніторингу Виконавця будується захищений канал.

Варіанти організації:

— На базі мережевого обладнання Замовника та мережі Інтернет з використанням віртуальних приватних мереж (IPSec VPN).

— На базі програмно-апаратного комплексу Виконавця та мережі Інтернет з використанням віртуальних приватних мереж (IPSec VPN).

Канали зв’язку до мережі Інтернет та необхідний пул IP-адрес надаються Замовником. У окремих випадках можуть використовуватися виділені канали

зв’язку. Необхідність резервування каналів зв’язку визначається в залежності від вимог Замовника.

- Організація передачі даних до програмно-апаратного комплексу Замовником

Налаштування активів у якості джерел подій інформаційної безпеки здійснює Замовник враховуючи рекомендації/інструкції Виконавця відповідно до обраного/обумовленого пакету послуг. Передача даних налаштовується з врахуванням лише потрібних даних, на базі яких буде проводитися аналіз і моніторинг подій інформаційної безпеки.

Наступним етапом йде створення правил виявлення інцидентів.

Виявлення подій інформаційної безпеки у процесі моніторингу відбувається шляхом аналізу даних або повідомлень від сенсорів. Даний аналіз відбувається в системі управління подіями інформаційної безпеки (SIEM, SOAR, із джерел або іншими засобами Виконавця) відповідними правилами кореляції. Правила є попередньо налаштованими у SIEM та створеними на вимогу Замовника чи за рекомендацією Виконавця для покращення функціонування SIEM/SOAR.

Для коректного налаштування використання правил потрібні тестова експлуатація та накопичення статистики типового стану мережі Замовника (1-3 міс. в залежності від мережі). Приблизний перелік включає:

— аудит подій входу до системи – кількість входів за одиницю часу, кількість вдалих входів, невдалих спроб, причини невдалих спроб;

— аудит керування обліковими записами: створення, видалення облікового запису, зміна паролів чи інших атрибутів автентифікації, як на рівні операційної системи, так і на кожному з сервісів, де є автентифікація;

— кількість унікальних IP–адрес, з яких надходять запити;

— кількість запитів, що надсилаються на адресу певного ресурсу;

— швидкість трафіку на мережевому інтерфейсі, загальна за протоколами, за адресами «внутрішніх» хостів;

— кількість запитів до ресурсу за типами запитів та ідентифікаторами ресурсу (URI);

— кількість невиконаних запитів, за типами помилок тощо;

— фіксування повторюваних записів, які встановлюються за замовчуванням для Замовника;

— налаштування/створення правил у відповідності до обумовлених вимог моніторингу;

— корегування правил кореляції з метою зменшення кількості хибних спрацювань та організації більш ефективного процесу моніторингу (1–3 міс).

Правила кореляції потребують змін або створення нових в залежності від інфраструктури Замовника та об`єктів, щодо яких здійснюється моніторинг, появи нових вимог до моніторингу чи появи нових загроз. У подальшому процес коригувань та додаткових налаштувань залежатиме від змін, які будуть впроваджуватися в інфраструктуру Замовника (оновлення ОС, оновлення ПЗ, впровадження додаткових сервісів, засобів захисту тощо).

2.1.2 Виявлення та аналіз інцидентів

Кожному мережевому сервісу, що підлягає моніторингу, складається перелік параметрів, які спостерігаються (включені у моніторинг) на основі зафіксованих правил та типової поведінки мережі Замовника. Слід враховувати, що одна подія може породжувати інцидент, але для кожного інциденту є перелік подій, які є доброякісними. Усі події, що відбуваються в мережі Замовника, мають зберігатися у сховищі Замовника (іноді Виконавця – за домовленістю) впродовж певного проміжку часу та є джерелом створення нових правил для моніторингу, перевірки можливих загроз у разі виникнення таких, а також підлягають розслідуванню та аналізуванню аналітиками Замовника.

У разі виявлення відхилень поведінки мережі/появи нетипових подій, що надходять до SIEM/SOAR та відповідають правилам кореляції, система фіксує

інцидент, надає йому відповідний пріоритет та очікує на вирішення. Інформація про виявлений інцидент має бути зафіксована, доступна та містити:

- ID.
- Пріоритет.
- Вплив.
- Час реєстрації.
- Реєстратор (джерело).
- Метод інформування про інцидент.
- Опис.
- Статус – статус, який присвоюється інциденту в SIEM: новий, в роботі, в режимі очікування, вирішений, закритий.
- Пов'язані інциденти (проблеми/відома помилка).
- Час прийняття рішення.
- Час закриття.

У загальному випадку, ознаки інциденту поділяються на дві основні категорії – повідомлення про те, що інцидент відбувається в даний момент часу, і повідомлення про те, що інцидент, можливо, відбудеться у майбутньому.

Події інформаційної безпеки в автоматичному режимі частково фіксуються як інцидент, частково – потребують аналізу оператора Виконавця і в подальшому можуть класифікуватися, як інцидент, помилкове спрацювання та інше. Інциденти фіксуються в SIEM/SOAR та призначаються для розслідування аналітикам Виконавця у випадку повернення на доопрацювання із залученням експерта Замовника, якщо подія, що виникла, є нетиповою.

Під час розслідування, аналітиком аналізується додаткова інформація, пов’язана з інцидентом та може бути затребувана інформація від відповідальних осіб Замовника. Усі дії та час аналітика фіксуються в SIEM.

Також проводиться поглиблений аналіз інциденту, розробляються висновки і надаються рекомендації Замовнику з підвищення інформаційної безпеки та реагування на інциденти. Формується звіт про інцидент з наданням

рекомендації, розроблених на етапі аналізу: внутрішні – корегування, створення правил SIEM; зовнішні – надання рекомендацій Замовнику із захисту мережі.

Аналітичний звіт повинен містити комплексне та поглиблене розслідування інцидентів з повним повторним встановленням їх хронології, що включає підтримку реагування, детальний аналіз постраждалих активів та ретроспективний аналіз подій ІБ.

Пріоритизація інцидентів інформаційної безпеки базується на таких основних чинниках:

- потенціал загрози – теперішній і потенційно можливий ефект інциденту інформаційної безпеки. Розглядається не тільки факт доконаного інциденту, а й наслідки та потенційні загрози, які можуть виникнути в подальшому;
- ймовірності реалізації ризику і критичність постраждалих систем – критичність залучених в інцидент активів.

Таким чином, кореляція цих показників дає підстави експертам команди реагування робити висновки про пріоритети інцидентів.

Для кожного типу інциденту встановлюються відповідні рівні критичності, автоматично на основі індивідуальних правил чи власноруч, та часові нормативи для розслідування, при перевищені яких відбувається ескалація інциденту в системі.

Пріоритет встановлюється в SIEM з врахуванням наступних критеріїв:

- Терміновість.
- Вплив на бізнес.
- Небезпека для функціонування Замовника.
- Обсяг послуг.
- Фінансові збитки.
- Вплив на ділову репутацію.
- Вплив на дотримання законів та інших норм.

Рівні критичності (Табл. 2.2) та дії операторів/аналітиків можуть корегуватися за погодженням із Замовником.

Таблиця 2.2 – Рівні критичності інциденту

Пріоритет	**Опис**
Критичний	Вихід системи з ладу. Неможливість виконувати будь-який важливий бізнес-процес. Високий вплив на процеси Замовника та суттєвий збиток.
Високий	Значна частина функцій системи не виконується або спостерігається значне зниження продуктивності системи в цілому. Високий вплив на процеси Замовника та суттєвий збиток.
Середній	Зниження продуктивності системи, несправності однієї або декількох системних функцій. Незначний вплив на системи Замовника. Спостерігається вплив на продуктивність бізнес–процесів, що може привести до збитку.
Низький	Незначний вплив на бізнес-процеси Замовника. Збиток відсутній.
Мінімальний	Не впливає на бізнес-процеси Замовника. Збиток відсутній.

Замовник надає Виконавцю таблицю (Табл. 2.3) з переліком його систем, сервісів, облікових записів тощо, для яких встановлено рівень критичності при виникненні інциденту.

Таблиця 2.3 – Приклад визначення рівня критичності сервісів Замовника

Сервіси, служби та системи Замовника, які потребують моніторингу	**Критичність**
Серверні операційні системи (Windows Server, Cisco Application Deployment Engine OS Release: 3.0 (Linux), Cisco Fire Linux, Cisco Linux та ін.)	Високий
Сервери (контролер домену, поштовий сервер, проксі-сервер, Web-сервер та ін.)	Високий
Мережеві пристрої (мережеві екрани, маршрутизатори, комутатори)	Високий
Мережеві порти TCP/22 UDP/137	Високий
Мережеві протоколи (MAC, IP, ICMP, TCP і UDP, HTTP, FTP, POP3 і SMTP, SSH)	Високий
Бази даних (клієнт-серверна, файл-серверна)	Високий

Хости (внутрішній, зовнішній)	Високий
Служби каталогів (Active Directory)	Високий
Облікові записи (привілейований, адміністратора, персональний, гостьовий, стандартний користувач, сервісний, локальний, доменний)	Високий
Хмарні сховища даних (Dropbox, iCloud, OneDrive, Google Drive)	Середній
Політики безпеки (локальна, групова)	Середній
Оновлення ПЗ (автоматичне, критичне)	Низький
Мережеві ресурси (принтери, факси, модеми)	Низький

Сповіщення про інцидент містить наступну інформацію:

- номер Інциденту в SIEM;
- дата та час фіксації Інциденту;
- пріоритет;
- агент, що зафіксував Інцидент;
- детальний опис проблеми;
- рекомендації щодо її усунення.

В якості основного каналу комунікації використовується Електронна пошта (інтегрована з системою SOAR).

Альтернативні джерела:

- Месенджери.
- Голосове повідомлення.
- Телефонні дзвінки.

За відсутності доступу до корпоративної електронної пошти передача інформації про Інцидент здійснюється співробітниками SOC через альтернативні канали, визначені Договором.

Сповіщення Замовника виконується автоматично та/або співробітниками під час реєстрації інциденту відповідно до Договору та згідно пріоритету через визначені канали інформування.

Сповіщення Виконавця виконуються при:

- опрацюванні інциденту;

- нейтралізації, відновленні після інциденту – надання зворотного зв’язку;
- змінах на мережі, що впливають на моніторинг.

2.1.3 Локалізація, нейтралізація та відновлення

Локалізація інциденту – ряд заходів та дій, націлених на виявлення периметру дії інциденту, на обмеження та запобігання її розповсюдженню за межі периметру інфраструктури Замовника, а також переривання впливу на мережу та системи Замовника.

Виконання дій з локалізації здійснюється відповідно до зони відповідальності працівника SOC, власників та адміністраторів систем.

Критерії визначення відповідних дій з локалізації включають:

- потенційний збиток;
- потреба в збереженні доказів;
- доступність послуги (наприклад, підключення до мережі, послуги, що надаються стороннім сторонам);
- час та ресурси, необхідні для реалізації стратегії;
- ефективність дій;
- тривалість прийняття.

Виконавець надає Замовнику рекомендації щодо наступних дій з локалізації інциденту:

1. Попереднє налаштування граничних пристроїв для запобігання зараження однієї системою інших.

2. Автоматичне або дистанційне від'єднання зараженого комп'ютера/системи від мережі для того, щоб запобігти зараженню інших комп’ютерів, а також унеможливити вчинення зловмисником несанкціонованих дій на зараженому комп'ютері (шкідливе ПЗ може, наприклад, виконувати розсилку спаму, використовувати комп'ютер для проведення DDoS-атак, зберігати на ньому нелегальні файли і т.д.).

3. Ізоляція залучених в інцидент хостів на мережевому рівні.

4. Зміна конфігурації брандмауера та маршрутизатора, щоб зупинити мережевий трафік, який є частиною інциденту, DDoS атаки.

5. Зміна списків контролю доступу.

6. Спрямування зловмисника до пісочниці (мережі-приманки, хости-приманки), щоб стежити за діяльністю зловмисника, як правило, для збору додаткових доказів.

7. За необхідності, надсилання підозрілих файлів в антивірусні компанії, з якими працює Компанія, щоб визначити, чи дійсно вони є шкідливими програмами (слід заархівувати файли в zip–архів з паролем).

На етапі нейтралізації Замовнику слід видалити всі компоненти, пов’язані з інцидентом, усі артефакти, залишені зловмисником (шкідливий код, дані тощо), та закрити кожну вразливість, яку зловмисник використовував в першу чергу для вторгнення.

Під час видалення необхідно ідентифікувати всі порушені хости Замовника, щоб їх можна було виправити. У деяких випадках ліквідація або не потрібна, або виконується під час відновлення.

Процедура усунення наслідків інциденту включає інформування Замовника про загрозу та/або надання йому інструкцій/рекомендацій щодо подальших дій, а саме:

1. Видалення виявлених індикаторів компрометації і слідів присутності шкідливого ПО/зловмисників.

2. Видалення шкідливих програм.

3. Визначення та нейтралізація всіх вразливих місць, які були використані.

4. Вимкнення порушених облікових записів користувачів.

5. Запуск вірусного або шпигунського сканера для видалення файлів і служб зловмисника.

6. Зміна паролів порушених облікових записів користувачів.

7. Зміна профілів захисту ЗЗІ.

8. Контроль за повнотою виконання дій з боку залучених підрозділів і відсутністю повторної компрометації систем зловмисниками.

9. Оновлення сигнатур.

10. Перезаливка заражених хостів.

11. Установка останніх оновлень і вироблення компенсаційних заходів для усунення критичних вразливостей, використаних при атаці.

12. За необхідності, передача даних відповідальній для інформування зовнішніх зацікавлених сторін, таких як ЗМІ.

Згідно умов Договору між Замовником та Виконавцем, інженери та аналітики SOC надають рекомендації щодо відновлення після інциденту – відновлення системи (систем) Замовника, щоб повернутися до нормальної роботи та усунути вразливості для запобігання виникнення подібних інцидентів. Існує кілька способів відновлення після інциденту кібербезпеки.

План з відновлення включає наступні компоненти:

- розрахунковий час для відновлення,
- стратегії відновлення діяльності Замовника в найшвидший термін,
- опис основних ресурсів, обладнання та персоналу, необхідних для відновлення операцій Замовника.

Відновлення слід здійснювати поетапно. Під час відновлення адміністратори Замовника відновлюють системи до їх нормальної роботи, підтверджують, що системи функціонують нормально. Співробітники Замовника відповідно до зони відповідальності та рекомендацій Виконавця усувають вразливості для запобігання виникнення подібних інцидентів згідно умов Договору між Замовником та Виконавцем.

Дії Замовника, спрямовані на відновлення інфраструктури після інциденту:

1. Для відновлення системи використовувати тільки незаражені резервні копії – перевіряти резервні копії системи на наявність вірусів, руткітів та фонових сайтів, перш ніж відновити її.

2. Якщо не знайдено надійного резервного копіювання, то систему потрібно відновити з нуля.

3. Замінити компрометовані файли на чисті версії.

4. Після відновлення системи потрібно усунути вразливості, які дозволили зловмиснику отримати доступ до системи:

- встановити патчі,
- змінити паролі,
- змінити облікові записи,
- посилити захист мережевого периметру,
- змінити набори правил брандмауера,
- змінити список контролю доступу до граничних маршрутизаторів та ін.

5. Застосувати більш високий рівень реєстрації системи та моніторингу мережі.

6. Перевірити, чи всі функції працюють належним чином.

7. Необхідним є ведення журналу або моніторингу мережі. Після того, як ресурс успішно атакується, його часто атакують знову, або інші ресурси в організації атакуються аналогічним чином.

На етапі розслідування за необхідності проводиться розслідування критичних інцидентів, яке допомагає оцінити прогалини в поточній стратегії безпеки і знайти способи, як їх виправити.

У Замовника призначається відповідальна особа, яка координує дії всіх підрозділів в рамках розслідування інциденту. Цей фахівець повинен мати повноваження і контакти всіх задіяних у розслідуванні співробітників. Як правило, цю роль виконує Керівник служби інформаційної безпеки Замовника. Залежно від серйозності інциденту до його розслідування можуть бути

підключені зовнішні організації, у тому числі Виконавець (за домовленістю) або спеціалісти-форензики – комп'ютерні криміналісти, які займаються розслідуванням кібер-злочинів.

У ході розслідування інциденту всі свідчення повинні бути захищені від дискредитації, оскільки дані можуть містити інформацію про дієві вразливості інформаційної системи. Розрізняють технологічні і операційні свідчення впливу. До технологічних свідчень відносять інформацію, отриману від технічних засобів збору та аналізу даних (сніфери, IDS), до операційних – дані або докази, зібрані в процесі опитування персоналу, свідчення звернень до служби техпідтримки.

За результатами проведення розслідування необхідно провести зустріч між Замовником та Виконавцем і на основі консолідованого звіту Замовника про результати проведеного розслідування підключити до SIEM нові джерела та змінити/оновити правила кореляції, а також обговорити стратегій та рекомендацій.

2.2 Загальний опис підходів до оцінки ефективності SOC

Для того, щоб оцінити ефективність роботи SOC на прикладі обраної організації, перш за все треба з'ясувати критерії та метрики, по яким це можна зробити.

Як зрозуміти, що послуги, що надаються центром моніторингу та реагування, відповідають очікуванням клієнтів? Як переконатись, що SOC регулярно працює над підвищенням своєї ефективності? Для цього необхідно оцінити внутрішні процеси та послуги SOC. Оцінка ефективності процесів і сервісів дозволяє організаціям прогнозувати результати зусиль, що додаються, визначати основні проблеми, що впливають на надання послуг, і надавати керівництву SOC можливість приймати поінформовані рішення про підвищення ефективності.

Для оцінки використовуються метрики, показники рівня обслуговування (SLI) та ключові показники ефективності (KPI). Метрики служать для

кількісного виміру, KPI визначають прийнятні значення ключових метрик в оцінці ефективності окремих внутрішніх процесів, а SLI визначають виміряні значення результатів обслуговування (тобто реальні цифри продуктивності сервісу), прив'язаних до угоди про рівень обслуговування (SLA). Якщо значення метрики потрапляє у діапазон заданого KPI, процес працює нормально. Вихід за межі діапазону вказує на знижену ефективність процесу чи можливу проблему.

У таблиці нижче (Табл. 2.4) представлені типи та призначення метрик, які зазвичай використовуються в центрах моніторингу та реагування.

Таблиця 2.4 – Типи та призначення метрик

Тип метрики	**Призначення метрики**	**Приклади**
Показник рівня обслуговування (SLI)	-Важлива метрика для вимірювання результатів обслуговування -Пов'язана з угодами про рівень обслуговування (SLA) -Основний критерій для оцінки результативності SOC	-Моніторинг безпеки -Консультування щодо загроз
Ключовий показник ефективності (KPI)	-Використовується для відстеження ключових аспектів під час виконання завдань SOC -Допомагає вимірювати результати процесу -Допомагає у прийнятті рішень	-Показник хибнопозитивних оповіщень -Кількість помилкових вердиктів аналітика
Метрики моніторингу	-Допомагає виявити проблеми ефективності -Вимірює поточний робочий стан -Допомагає прогнозувати проблеми	-Кількість оповіщень, оброблюваних кожним аналітиком -Сценарій використання, що знаходиться у розробці
Технічні метрики	-Вимірює ефективність інструментів SOC -Допомагає виявити проблеми виробничої потужності	-Використання пам'яті SIEM -Доступний простір сховища

	-Допомагає прогнозувати проблеми, пов'язані з технологічними процесами чи інструментами	

Важливо розуміти, що не для всіх метрик необхідно встановлювати значення KPI. Деякі з них, наприклад, метрики моніторингу, просто інформують про щось. Вони надають цінну інформацію про функціональні компоненти діяльності центрів моніторингу та реагування, а їхнє основне призначення – допомагати прогнозувати проблеми, які можуть знизити ефективність роботи.

В наступному підрозділі буде проведене вимірювання ефективності SOC ОД за деякими з вищезазначених критеріїв.

2.3 Вимірювання ефективності SOC

2.3.1 Кількість інцидентів

В якості вимірюваного діапазону був взятий проміжок часу у пів року (з 01.01.2023 до 30.06.2023).

В системі SOAR по всім клієнтам за цей час зафіксовано 98653 алертів, з яких було створено 11127 інцидентів (Рис. 2.1). Кількість інцидентів, що були закриті як фолспозітів (Рис. 2.2) – 8336 (що складає 75% від загальної кількості).

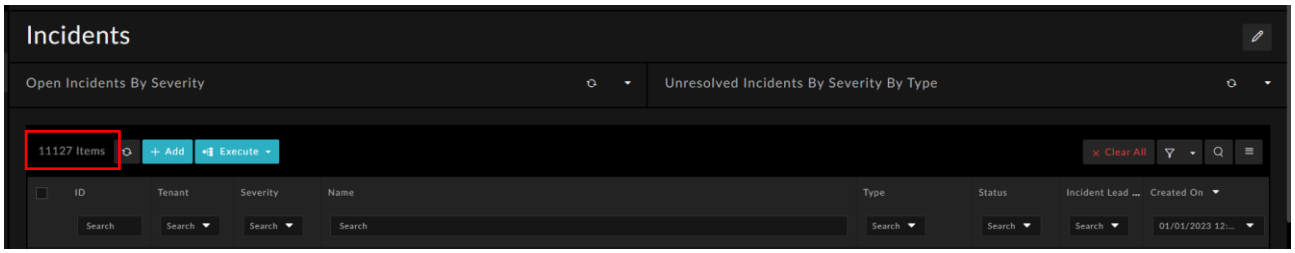


Рисунок 2.1 – Загальна кількість інцидентів за пів року

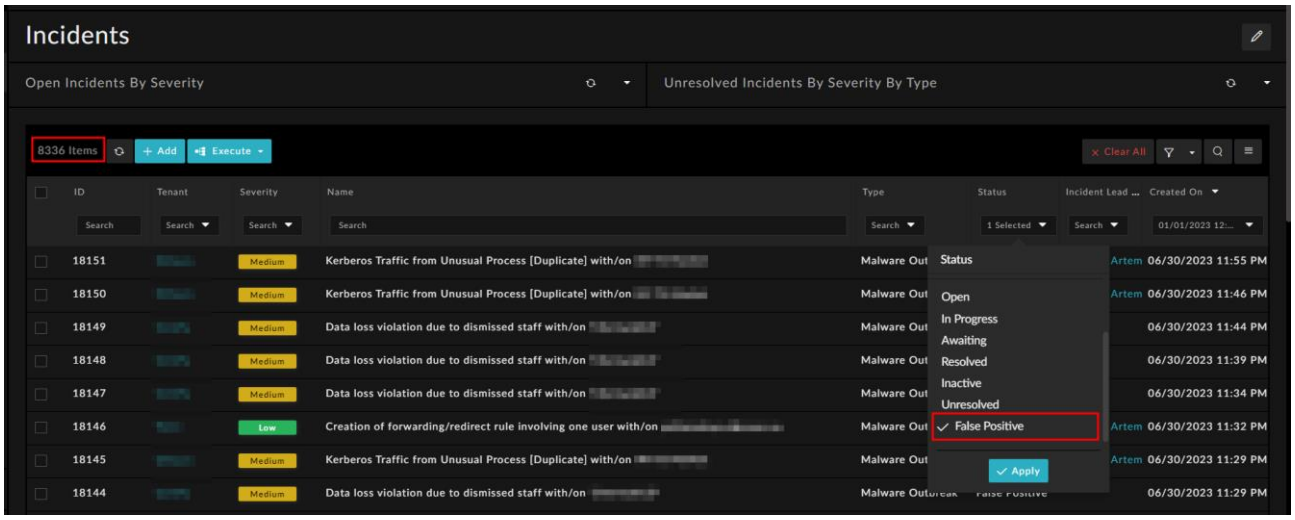


Рисунок 2.2 – Кількість фолспозітів спрацювань

Для більш детальної картини було взято одного з клієнтів (далі – «Замовник»), та розглянуто кількість і статус інцидентів, що були отримані з його підсистем (Windows, Network, Security, EndPoint, AntiVirus та ін.).

Загальні кількісні параметри обробки подій (спостережене проявлення в системі або мережі), алертів (подія, яка може бути небажаною або несанкціонованою) та інцидентів (що створені на основі алертів) за перше півріччя 2023 року можна побачити нижче (Рис. 2.3).

Рисунок 2.3 – Загальні кількісні параметри обробки подій, алертів та інцидентів

Обсяг інцидентів в системі SOAR по місяцям за період з 01.01.2023 до 30.06.2023 наведено на рисунку нижче (Рис. 2.4). Всього було створено 1200 інцидентів із 26568 зареєстрованих алертів. З них:

- за 337 інцидентами були проведені розслідування, а потім ці інциденти були закриті після обговорення з клієнтом;
- 863 були закриті на стороні Виконавця (SOC) з вердиктом false-positive.

Таким чином, за вказаний період команда Замовника та Виконавця у середньому обробляла близько 200 інцидентів різних статусів в місяць.

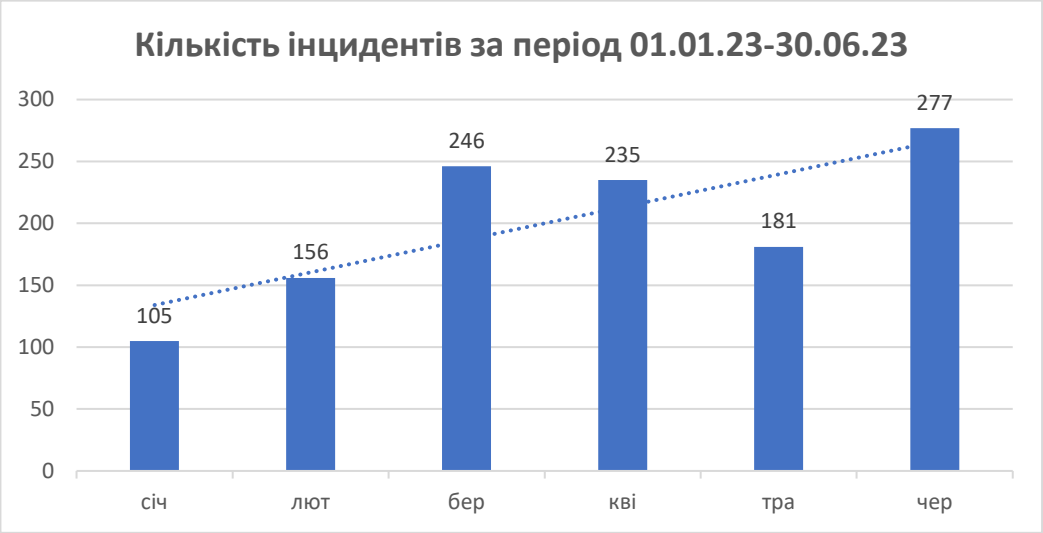
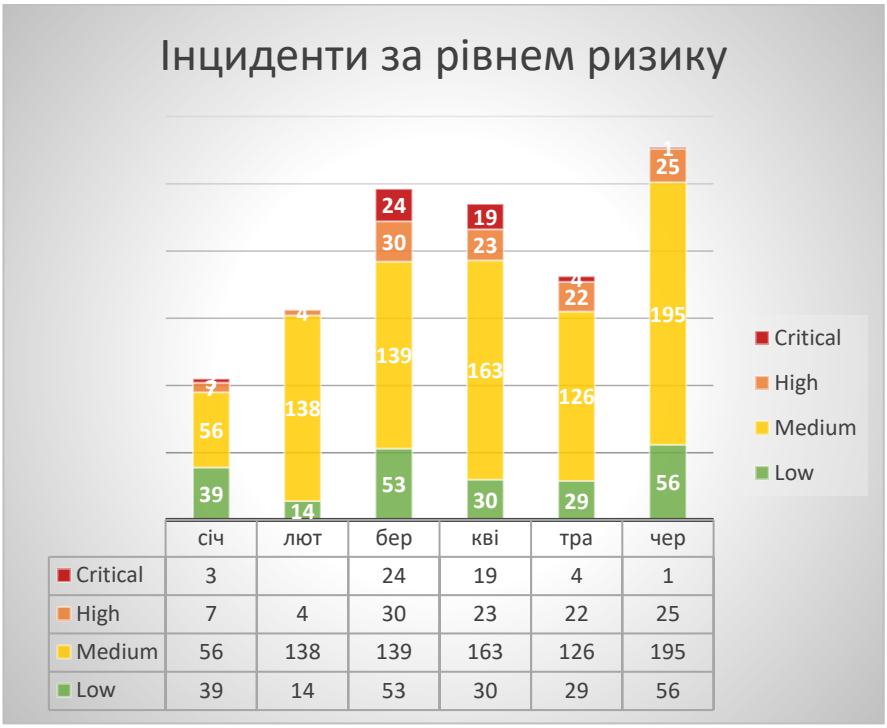


Рисунок 2.4 – Обсяг інцидентів по місяцям

Наступним кроком було проаналізувати рівень ризику інцидентів (Рис. 2.5), що надходили в SOAR.



	січ	лют	бер	кві	тра	чер
Critical	3		24	19	4	1
High	7	4	30	23	22	25
Medium	56	138	139	163	126	195
Low	39	14	53	30	29	56

Рисунок 2.5 – Інциденти за рівнем ризику

І останній пункт – зробити вибірку інцидентів за статусом (Рис. 2.6).

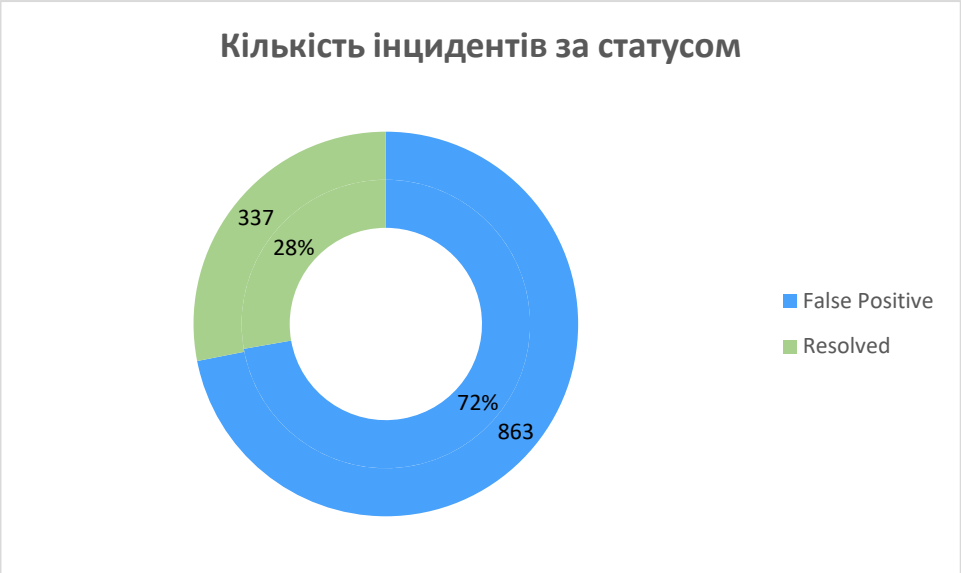


Рисунок 2.6 – Інциденти за статусом

Також слід зазначити, що частина спрацювань – автоматизовані (Рис. 2.7), а тому алерти по ним оброблюються і відправляються на клієнта у вигляді листа без участі операторів. За визначений проміжок часу на Замовника було відправлено 1818 листів, які були сформовані автоматично.

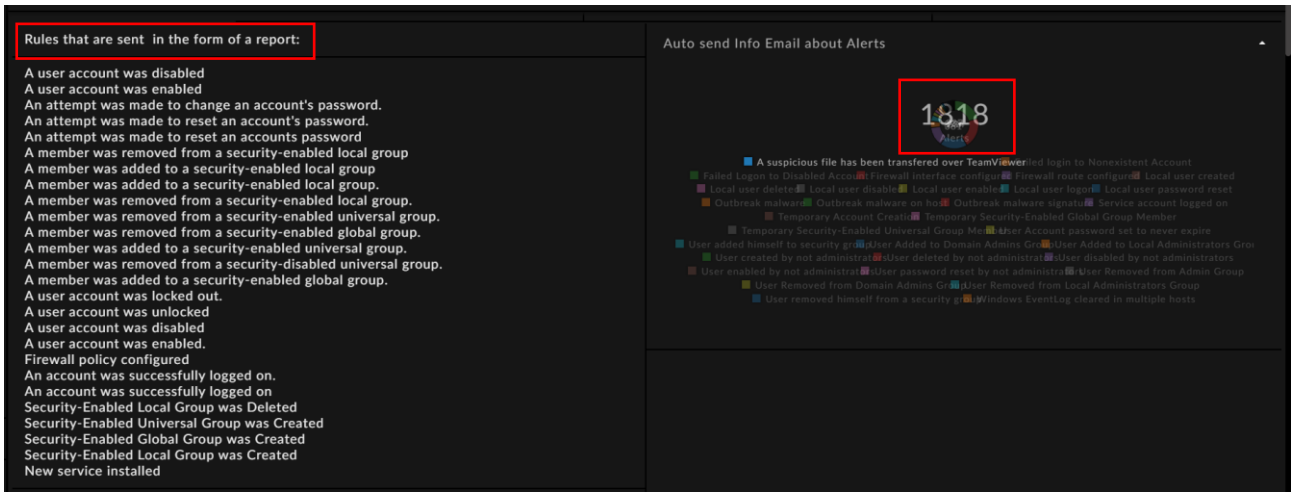


Рисунок 2.7 – Автоматизовані спрацювання

Проте, як можна помітити з діаграм вище, навіть незважаючи на автоматизацію, кількість інцидентів, що оброблюються вручну, все ще дуже висока.

2.3.2 Час реагування на інциденти

Якщо ми подивимося на часову шкалу будь-якого інциденту, то побачимо, що її можна розбити на декілька ключових точок (Рис. 2.8). Вона починається з моменту реалізації загрози, далі йде факт виявлення інциденту або загрози за допомогою використовуваних рішень (або за рахунок звернення користувача) та відправки до SOC відповідного сигналу тривоги. Продовжуючи, ми переходимо до моменту пріорітизації інциденту та його аналізу і обробки. Завершується часова шкала фактом закриття інциденту та усунення причин, що спричинили появу інциденту, який потрапив до центру моніторингу.

Загалом, життєвий цикл інциденту можна поділити на етапи Time-to-Detect, Time-to-Triage, Time-to-Contain.

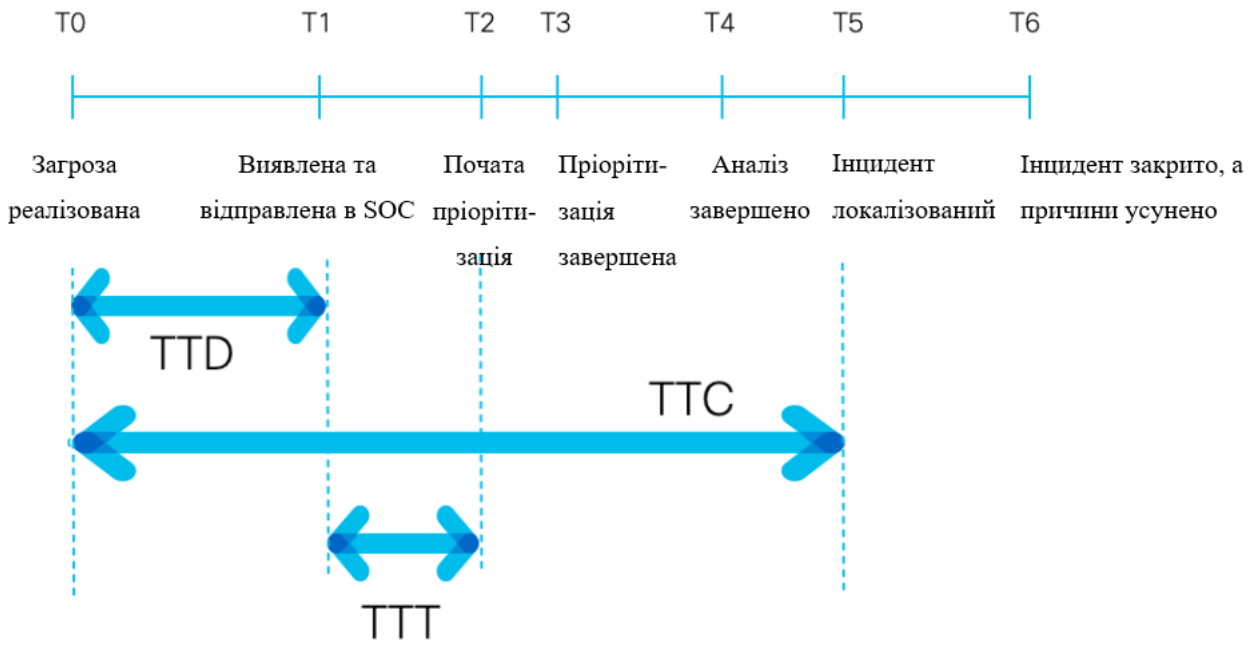


Рисунок 2.8 – Часова шкала інциденту

Для контролю першого етапу в системі SOAR були створені дашборди, які відслідковують час взяття алерту в роботу (Рис. 2.9). На них відображена інформація про кількість алертів, по яким був вихід за встановлені договором часові проміжки, та про аналітика першої лінії, який допустив цей вихід.

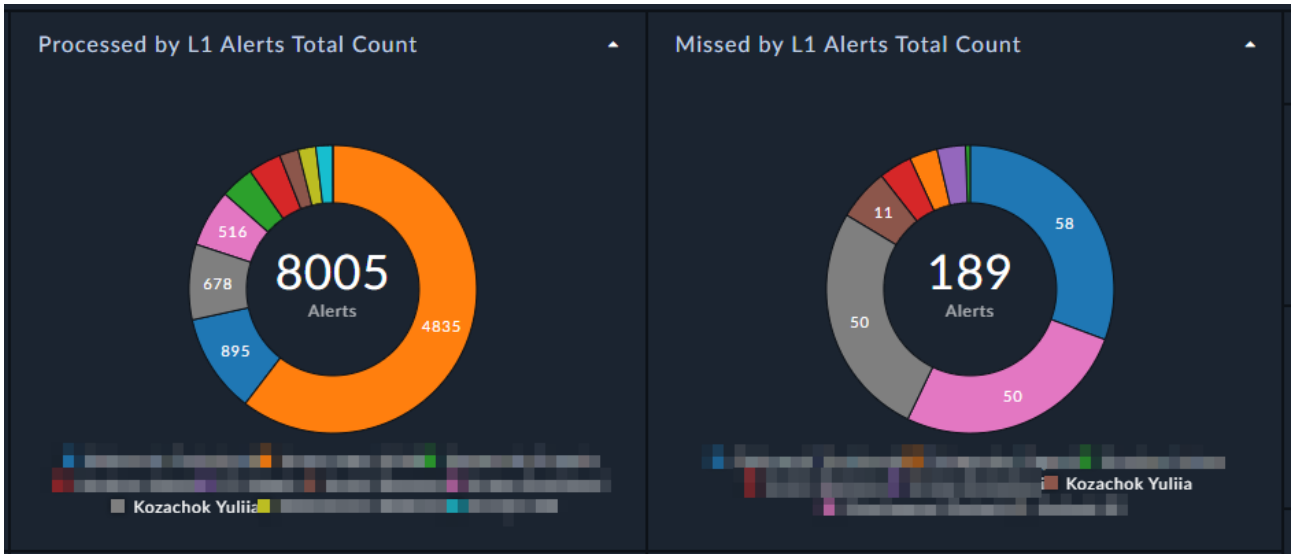


Рисунок 2.9 – Дашборди про взяті в роботу та пропущені алерти

Можна побачити, що за вибраний проміжок часу було пропущено 189 алертів, що становить всього 2,4% від загальної кількості. Враховуючи людський фактор, цей відсоток можна назвати досить малим.

Також на дашборді видно деталі про те, які саме алерти було пропущено (час, клієнт, назву та критичність спрацювання) кожним аналітиком L1 (Рис. 2.10).

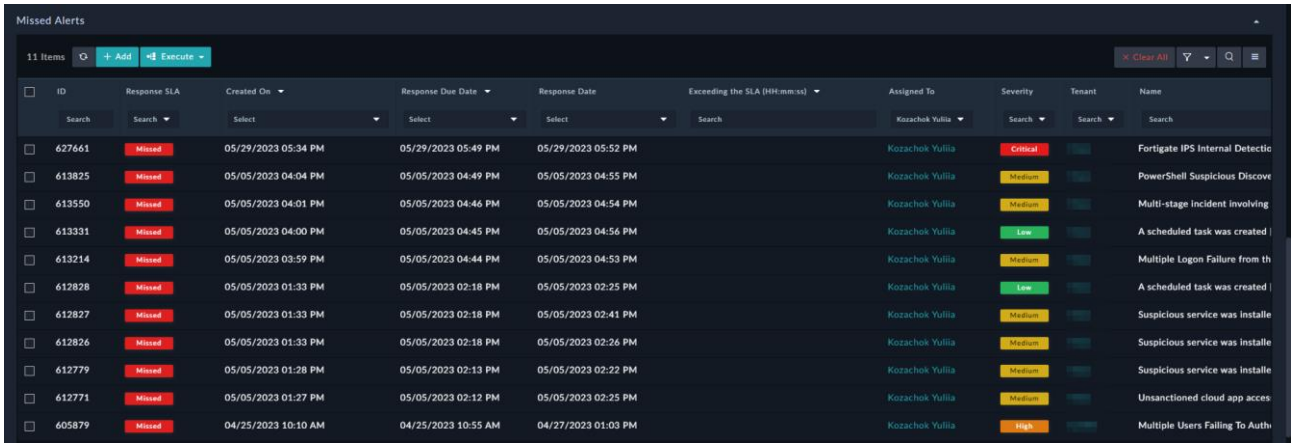


Рисунок 2.10 – Детальна інформація про пропуски

Контроль цих дашбордів дозволяє швидко виявляти виходи та з’ясовувати у аналітика L1 їх причини, щоб не допустити таких повторів у майбутньому.

2.3.3 Ескалація інцидентів

Ескалація інцидентів – це процес їх передачі від аналітиків L1 до аналітиків L2 з метою залучення додаткових ресурсів у тих випадках, коли інцидент перевищує можливості початкового рівня підтримки.

Процес ексалації реалізований через інтеграцію Microsoft Teams з SOAR. Для цього всередині інциденту треба натиснути на кнопку «Escalation» (Рис. 2.11), і сповіщення одразу ж буде надіслано у відповідний канал Teams (Рис. 2.12).

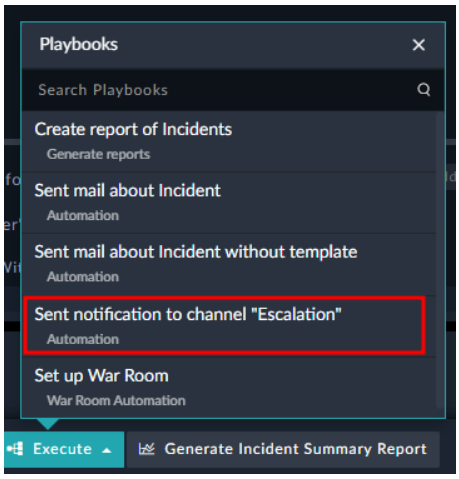


Рисунок 2.11 – Процес ескалації інциденту

Рисунок 2.12 – Сповіщення на каналі «Escalation» в Teams

Таким чином, якщо у аналітика першої лінії виникли труднощі з опрацюванням інциденту, в нього є можливість одразу ж передати його далі. У цій функції також передбачена можливість додати свій коментар до ескалації (Рис. 2.13), щоб L2 не витрачали додатковий час на початковий аналіз того, що ж трапилось.

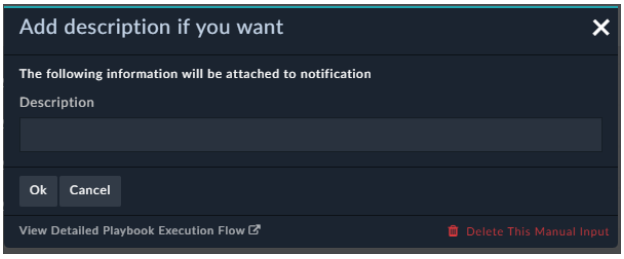


Рисунок 2.13 – Додавання опису до ескалації

Перш за все треба з’ясувати відсоток інцидентів, переданих аналітикам другої лінії (від L1 до L2). Ця метрика показує ефективність команди аналітиків першого рівня, що приймає на себе всі сигнали тривоги. Вищі значення цієї

метрики впливатимуть на команду L2 і можуть вказувати на низький рівень знань та компетенцій аналітиків L1, що говорить про потребу навчання співробітників цієї лінії SOC, а також про неефективний обмін інформацією.

Проаналізувавши канал Ескалації, відстежується закономірність, що в середньому за день ескалюється близько 5 інцидентів. Враховуючи загальну середню кількість створених за день інцидентів (близько 70), можна зробити висновок про високий рівень якості ескалації. Завдяки тому, що аналітики першої лінії передають на другу лінію тільки справді ті спрацювання, з якими треба розбиратися більш глибоко, останні мають можливість точно і якісно виконувати свою роботу.

Також слід зазначити, що аналітики L2 мають досить швидку реакцію на сповіщення про ескалацію (Рис. 2.14), що також значно скорочує загальний цикл життя інциденту.

Рисунок 2.14 – Час реакції аналітика L2 на ескалацію

2.4 Рекомендації по підвищенню ефективності SOC

На прикладі SOC «Октава Дефенс» було виконано оцінку ефективності існуючих засобів, рішень та способів ведення діяльності. Орієнтуючись на отримані результати та на загальні показники, можна надати наступні рекомендації по покращенню:

1. Зведення зайвого «шуму» до мінімуму

Результати аналізу в попередньому розділі показали, що в системі наявна дуже велика кількість фолспозітів спрацювань. Це заважає аналітикам, адже

відволікає їх від дійсно важливих інцидентів (які вони, більш того, можуть випадково пропустити в потоці шуму). Щоб вирішити цю проблему, треба по максимуму додати виключення в правила, щоб вони не спрацьовували на тих користувачів/процеси, що є легітимними.

2. Автоматизація процесів і процедур

Для того, щоб оператори не виконували роботу, яку може виконати «машина», треба зробити автоматичну обробку всіх інцидентів, які не потребують глибокого аналізу, а надають просто базову інформацію про те, що трапилось.

3. Написання плейбуків

Аналіз показав, що кількість спрацювань в цілому достатньо висока, і не менш важливим є те, що всі ці правила є досить різноманітними і унікальними. Написання плейбуків значно допомогло б аналітикам L1 тим, що пришвидшило б опрацювання інцидентів, адже значно легше обробляти їх по вже готовій інструкції.

4. Постійне підвищення кваліфікації персоналу

Персонал SOC повинен регулярно проходити навчання, щоб бути в курсі останніх тенденцій у сфері кібербезпеки, а також щоб мати достатній рівень знань, щоб не пропустити важливі спрацювання.

5. Впровадження нових інтеграцій

Інтеграції з новими платформами та рішеннями допоможуть ширше охоплювати моніторинг мережі замовника, а також підвищать якість роботи SOC.

6. Інвестування в технології

Такі технології, як системи моніторингу безпеки, системи виявлення вторгнень, системи реагування на інциденти, системи управління інформаційною безпекою та інші повинні бути сучасними та актуальними.

7. Регулярні оцінки ефективності

SOC повинен регулярно проводити оцінки своєї ефективності, що допоможе виявити недоліки в роботі та вжити заходів щодо їх усунення.

Впровадження цих рекомендацій допоможе SOC підвищити свою ефективність та захистити саму організацію та її клієнтів від кібератак.

РОЗДІЛ 3 – ПРАКТИЧНА РЕАЛІЗАЦІЯ РІШЕНЬ ПО ПІДВИЩЕННЮ ЕФЕКТИВНОСТІ SOC

3.1 Розробка автоматичної обробки спрацювань

На основі результатів аналізу з попереднього розділу було прийняте рішення про те, що необхідно налаштувати в SOAR автоматичну обробку тих спрацювань, які знаходяться в топі по рівню фолспозітіва та для яких не потрібен додатковий аналіз з боку операторів. Для цього треба розробити відповідний плейбук, кроки по створенню якого будуть представлені нижче.

1. Натискаємо «Automation» > «Playbooks» (Рис. 3.1) на панелі навігації ліворуч.

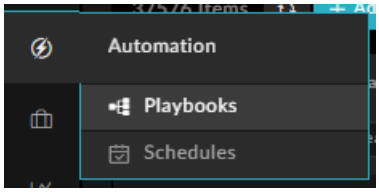


Рисунок 3.1 – Перший крок створення плейбуку

2. На вкладці «Playbooks Collections» (Рис. 3.2) натискаємо «New Collection» (1), щоб створити нову папку для зберігання плейбуків, або клацаєм на вже наявну папку і додаємо туди новий плейбук (2).

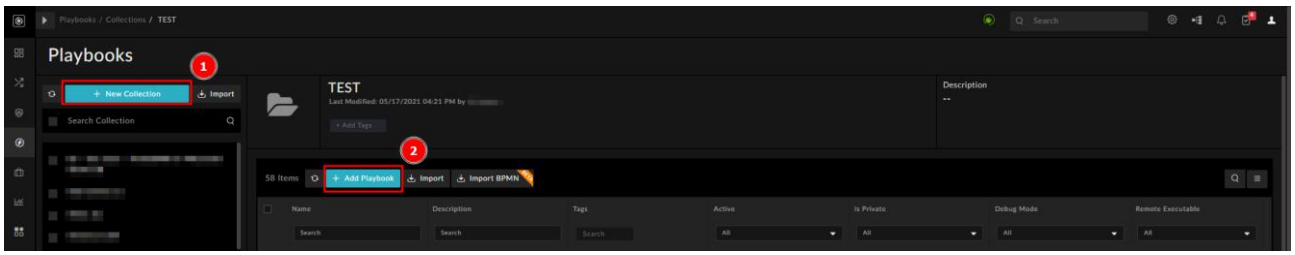


Рисунок 3.2 – Другий крок створення плейбуку

3. У діалоговому вікні «Add New Playbook» (Рис. 3.3) додаємо назву колекції в полі «Name» та, за бажанням, можна заповнити поле «Description». В нашому випадку плейбук буде мати назву «Auto create incident».

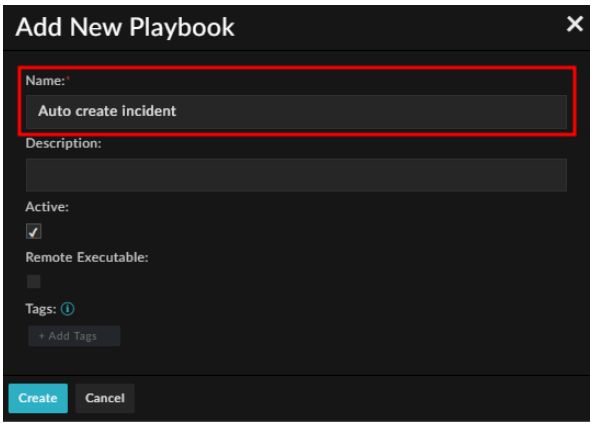


Рисунок 3.3 – Створення плейбуку

4. Наступним кроком FortiSOAR пропонує вибрати перший, тригерний крок, що вирішує, як буде розпочинатися плейбук (Рис. 3.4). В нашому випадку буде тригер типу «Referenced» (Рис. 3.5.), з відповідною назвою «Start».

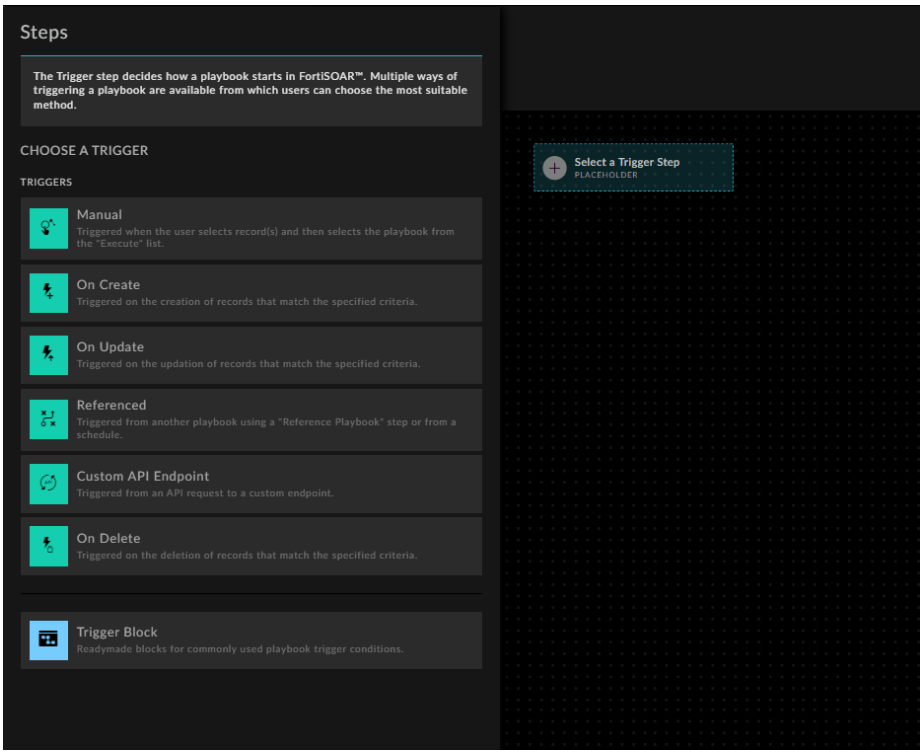


Рисунок 3.4 – Варіанти тригерів

Рисунок 3.5 – Перший крок плейбуку

5. Далі йде крок типу «Find Records», який було налаштовано (Рис. 3.6) так, щоб він шукав відповідні алерти в системі.

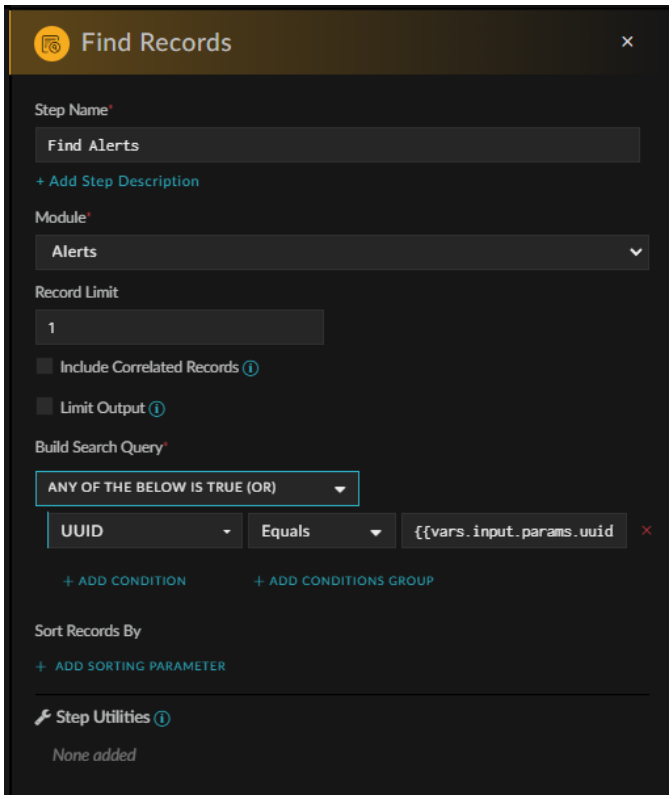


Рисунок 3.6 – Налаштування другого кроку

6. Потім ставимо крок типу «Decision», який буде здійснювати перевірку тенанта (клієнта) від якого прийшов алерт, і для якого прописуємо умову, у разі виконання (або, відповідно, невиконання) якої плейбук передбачає два можливі варіанти розвитку подій (Рис. 3.7).

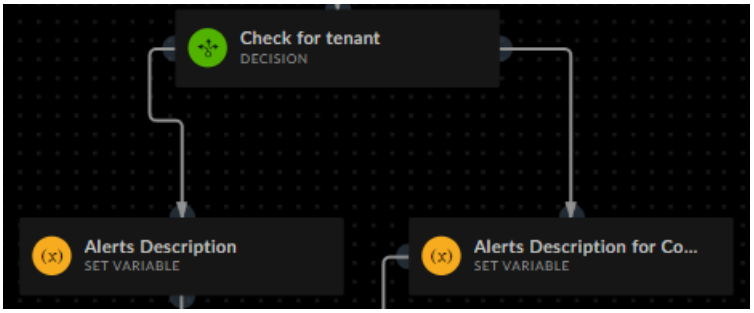


Рисунок 3.7 – Розгалудження схеми

Налаштування блоку «Decision» можна побачити нижче (Рис. 3.8)

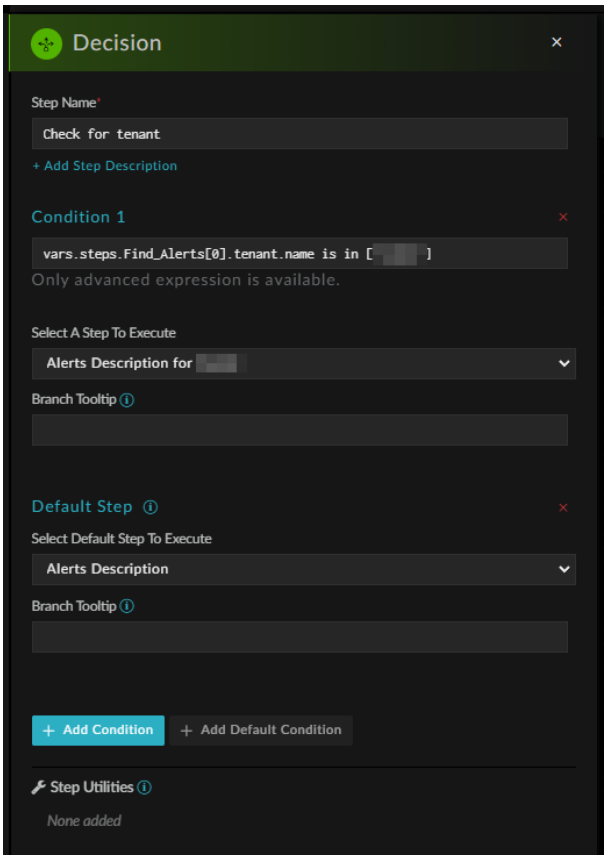


Рисунок 3.8 – Налаштування кроку «Decision»

7. Після того, як було обрано один з варіантів розгалудження, йде блок «Update Record», який вносить зміни до алертів, а саме ставить їм користувача «Autocreate SOAR» та змінює статус на «Investigating» (Рис. 3.9).

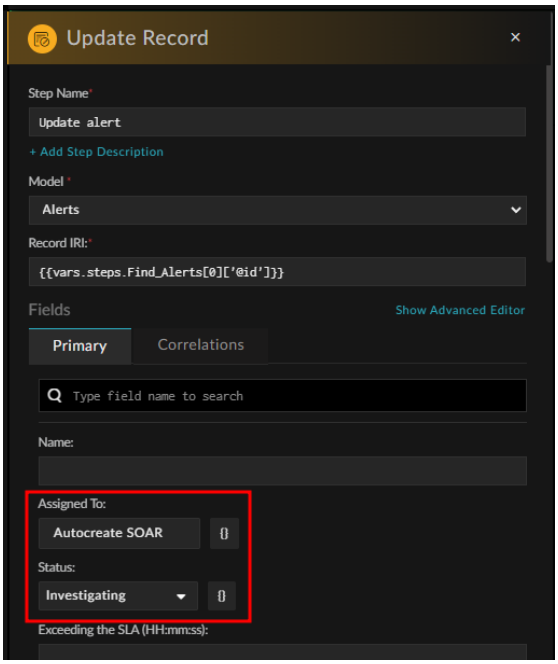


Рисунок 3.9 – Апдейт алертів

8. Далі йде блок, який відповідає за перевірку назви правила, по якому прийшов алерт. В ньому було задано 14 умов, в якості яких виступали 14 правил (три з яких можна побачити на Рис. 3.10), які було автоматизовано.

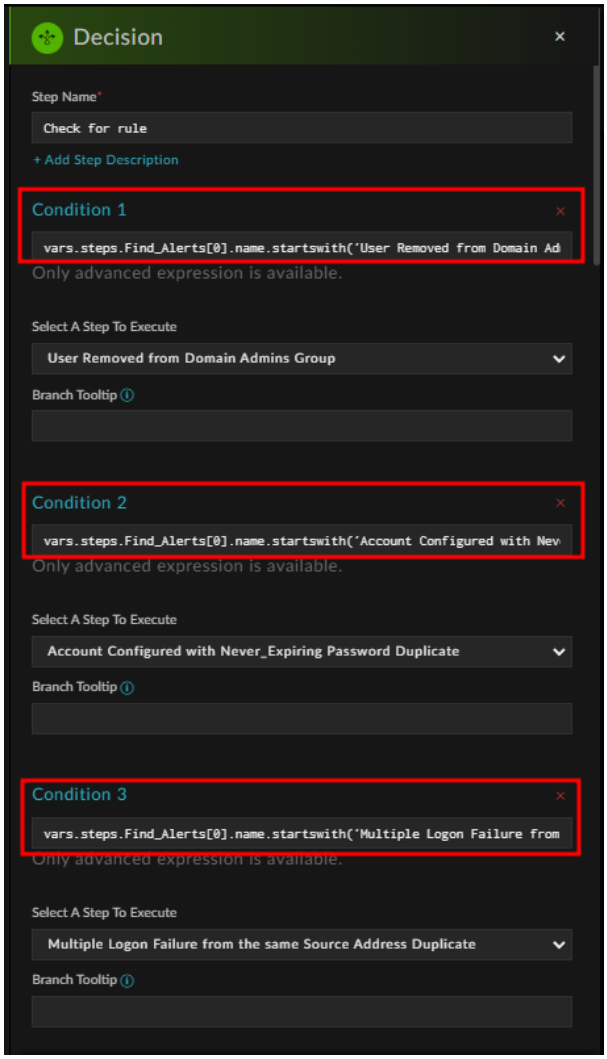


Рисунок 3.10 – Правила, що були автоматизовані

9. Наступним кроком для кожного з правил був налаштований блок (Рис. 3.11), який задавав текстове повідомлення, що буде відправлено на клієнта, та вказував, які поля повинні бути «підтягнуті» у цей опис, і яке поле виступає в якості «сутності» інциденту.

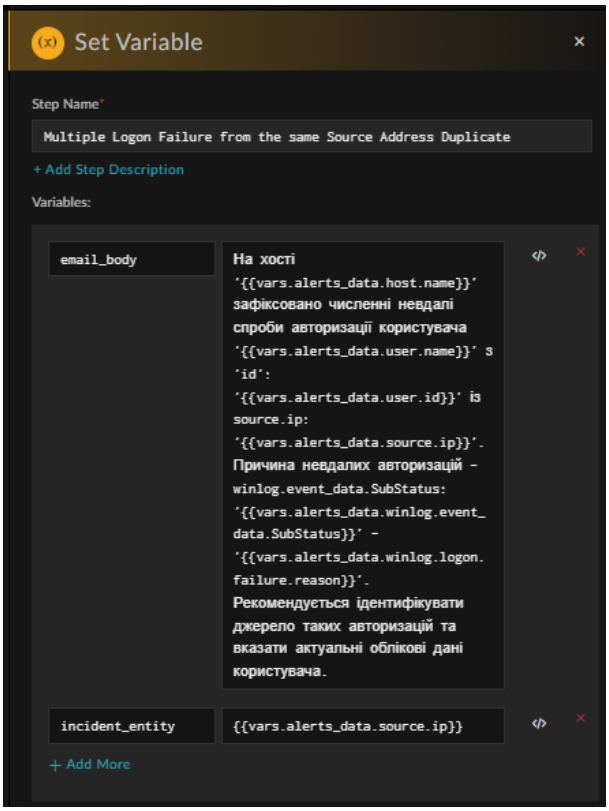


Рисунок 3.11 – Налаштування текстовки для одного з правил

10. Після цього було створено блок, який відповідає за пошук інцидентів, що відповідають заданим умовам (Рис. 3.13), і якщо всі з них правдиві – йде перевірка того, чи існує такий інцидент.

Потім можливі два варіанти розвитку подій (Рис. 3.12): якщо інцидент вже існує, то відбувається його апдейт; а якщо такого інциденту ще нема, то система його створює, і відправляє відповідний емейл на клієнта (Рис. 3.14).

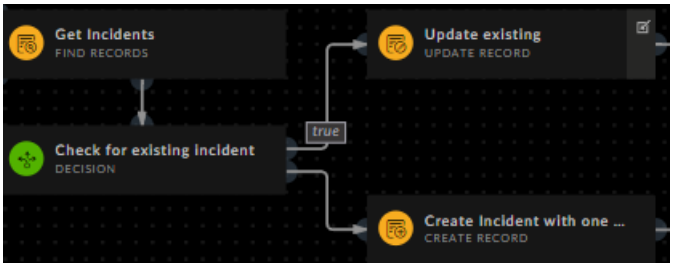


Рисунок 3.12 – Розгалудження схеми

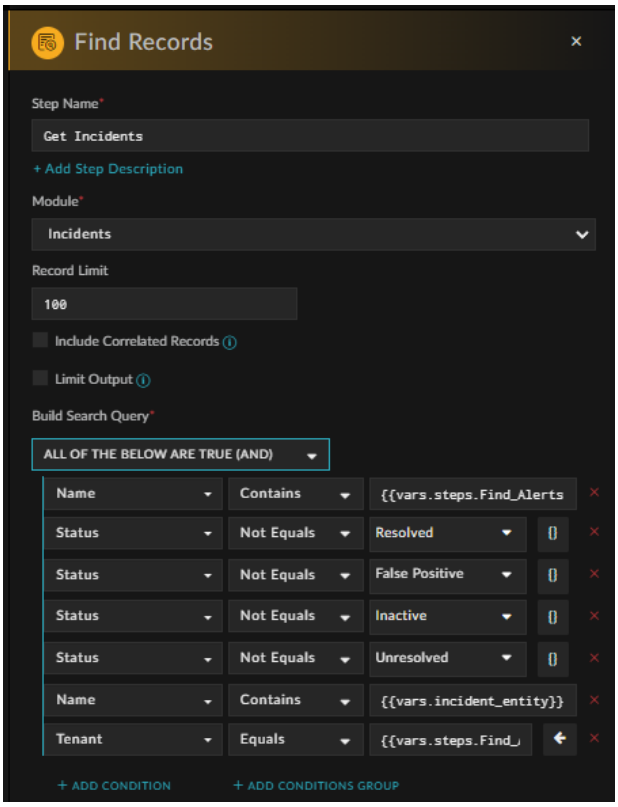


Рисунок 3.13 – Умови перевірки інциденту

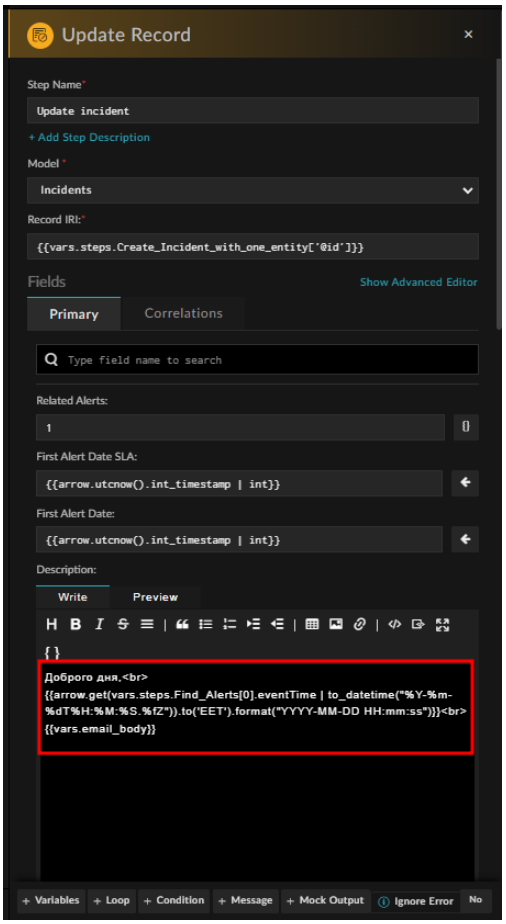


Рисунок 3.14 – Блок відправки емейлу

Загальний вигляд розробленого плейбуку можна побачити в Додатку А.

Після того, як плейбук був написаний, було перевірено його дієздатність на прикладі спрацювання правила «A scheduled task was created». Те, як у системі SOAR виглядає створений автоматично інцидент, продемонстровано нижче (Рис. 3.15).

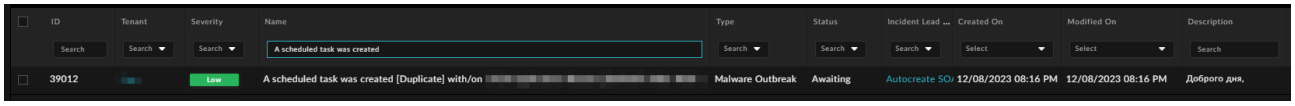


Рисунок 3.15 – Приклад автоматично створеного інциденту

Як бачимо (Рис. 3.16), в тіло листа, що був відправлений на замовника, прописаний саме той текст, що було задано в нашому плейбуці (1). Всі значення і поля підтягнулися коректно. Також видно, що в якості Incident Lead-а вказано користувача «Autocreate SOAR» (2), що каже саме на автоматичну обробку.

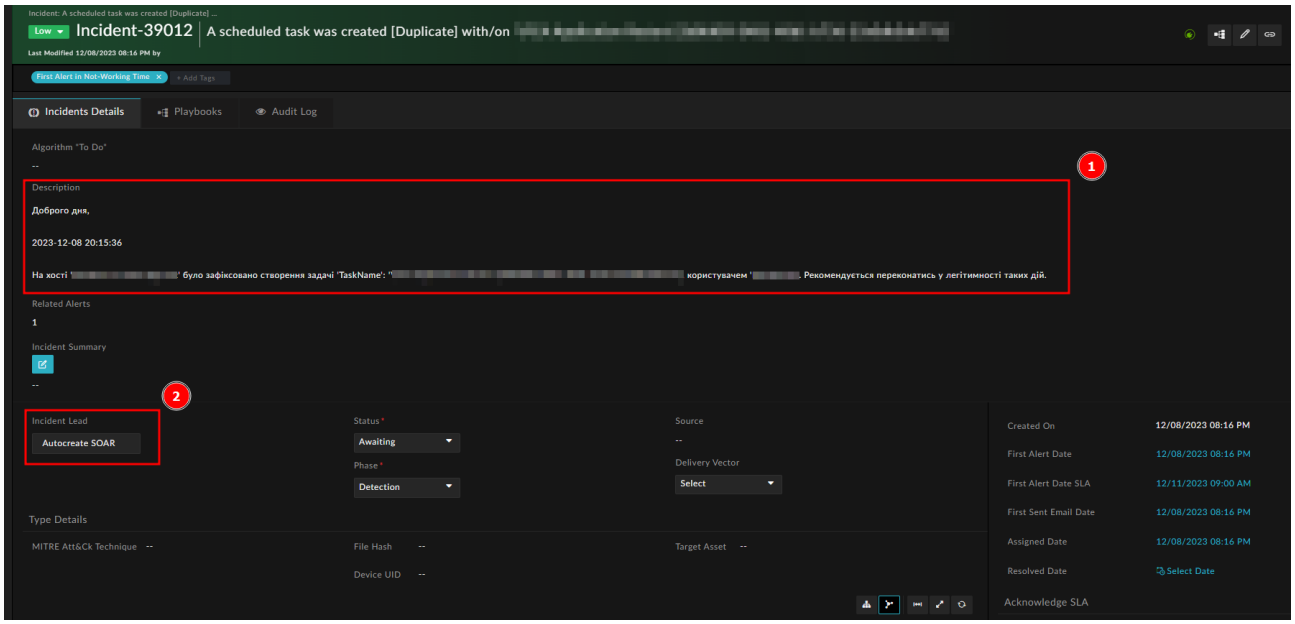


Рисунок 3.16 – Створений інцидент

Розробка цього плейбука значно спростить роботу аналітиків L1, адже тепер найчастіші хибнопозитивні сповіщення не будуть потребувати ручної обробки. Також це корисно тим, що замовники будуть давати зворотній зв’язок із проханням внести у виключення легітимні процеси/користувачів, адже в їх інтересах отримувати сповіщення тільки про трупозітів інциденти.

3.2 Налаштування інтеграції MISP з Elastic

Платформа MISP (Malware Information Sharing Platform) – це потужний інструмент, який кібераналітики можуть використовувати для обміну інформацією про шкідливе програмне забезпечення та інші кіберзагрози. MISP використовує стандартизований формат даних, який дозволяє кібераналітикам легко обмінюватися інформацією між собою та іншими організаціями.

Інтеграція MISP з Elastic може бути корисною з кількох причин:

1. Розширений аналіз загроз (Elastic надає потужні можливості для зберігання, індексації та аналізу даних, а отже е дозволить виконувати розширений пошук, аналіз та візуалізацію цих даних для отримання більш глибокого розуміння загроз безпеки).
2. Покращена кореляція та пошук (Elasticsearch може індексувати та зберігати дані, дозволяючи швидко здійснювати пошук, знаходження зв'язків та кореляцію між різними загрозами).
3. Полегшений процес виявлення загроз.
4. Візуалізація та звітність (Elastic Stack включає інструменти для візуалізації даних через Kibana, що дозволяє створювати звіти, графіки та діаграми на основі даних з MISP).
5. Автоматизація та вдосконалення реакції на загрози (за допомогою Elastic можна налаштувати автоматичну обробку та реагування на виявлені загрози, які базуються на даних з MISP, що дозволяє забезпечити більш швидку та ефективну реакцію на них).

Для того, щоб налаштувати цю інтеграцію, першим кроком необхідно у розділі «Administration» у налаштуваннях MISP згенерувати ключ API для взаємодії з Elastic. Потім треба відкрити Elastic відповідного замовника, перейти у розділ «Integrations» та знайти ту, що нас цікавить (Рис. 3.17).

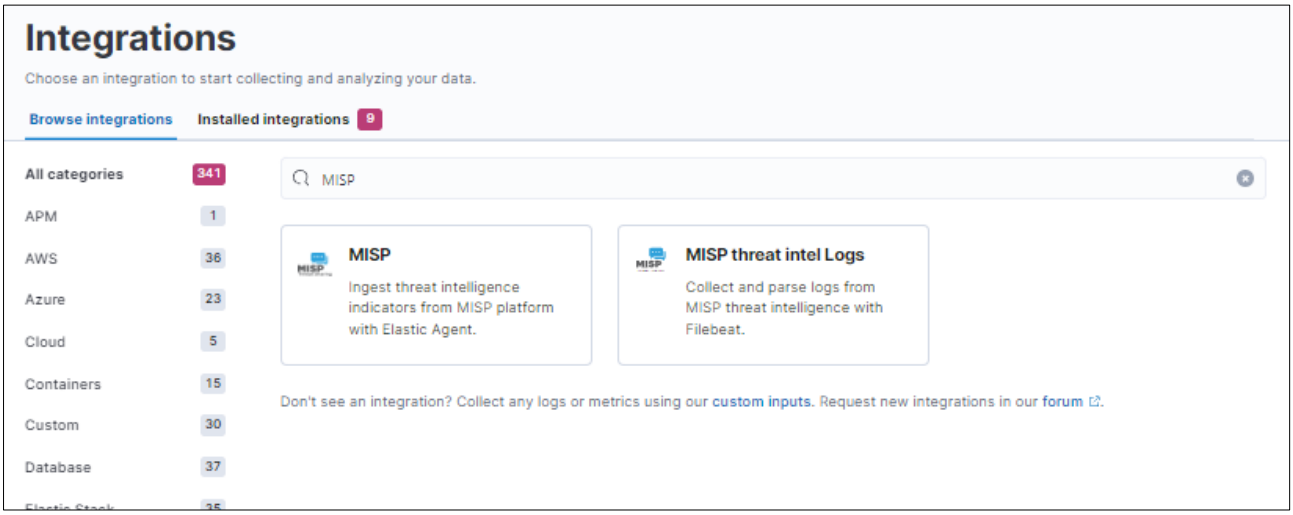


Рисунок 3.17 – Інтеграція MISP

Далі вставляємо згенерований ключ в поле «MISP API Token» (Рис. 3.18) та заповнюємо необхідну інформацію (таку як URL-адреса або ім’я хоста примірника MISP; інтервал, з яким будуть підвантажуватися логи; інтервал того, на який час назад буде здійснюватися пошук індикаторів).

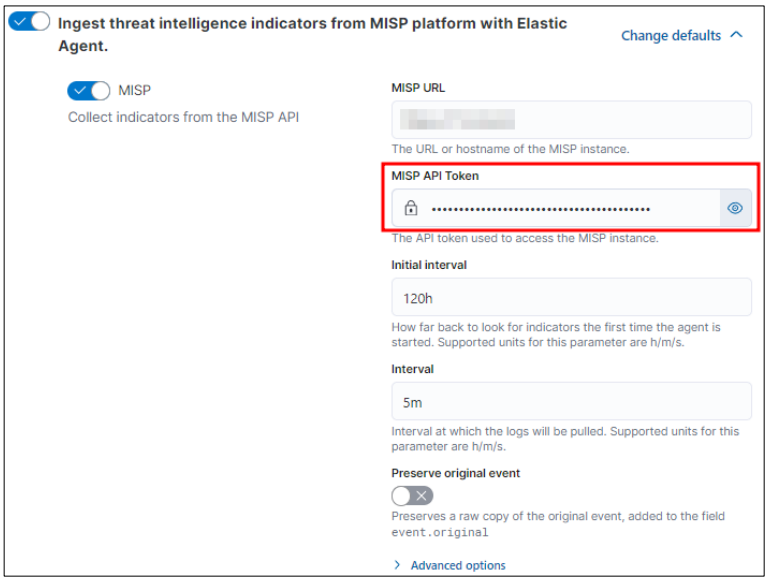


Рисунок 3.18 – API токен

Наступним кроком необхідно увімкнути вбудоване правило Elastic, що відповідає за цю інтеграцію. Для більшої зручності правило було поділене на три різних спрацювання (Рис. 3.19): збіг по хешу, по IP-адресі і по URL.

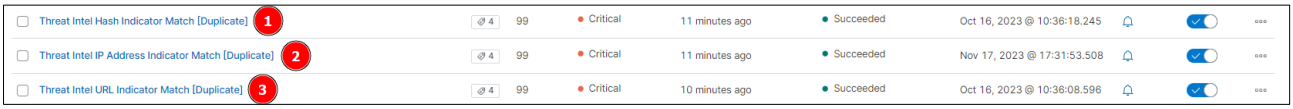


Рисунок 3.19 – Правила Elastic

Для прикладу розглянемо логіку одного з них, а саме того, що стосується хешів (Рис. 3.20). При його написанні було обрано тип правила «Indicator Match» (1), який відповідає за використання індикаторів з різних джерел (в нашому випадку з MISP) і їх співставлення з відповідними алертами та подіями. Далі було обрано індекс-паттерни, що нас цікавлять (2), прописано безпосередньо саму логіку правила (3), заповнені поля «Indicator index patterns» (4), «Indicator index query» (5), та обрано фільтри (6).

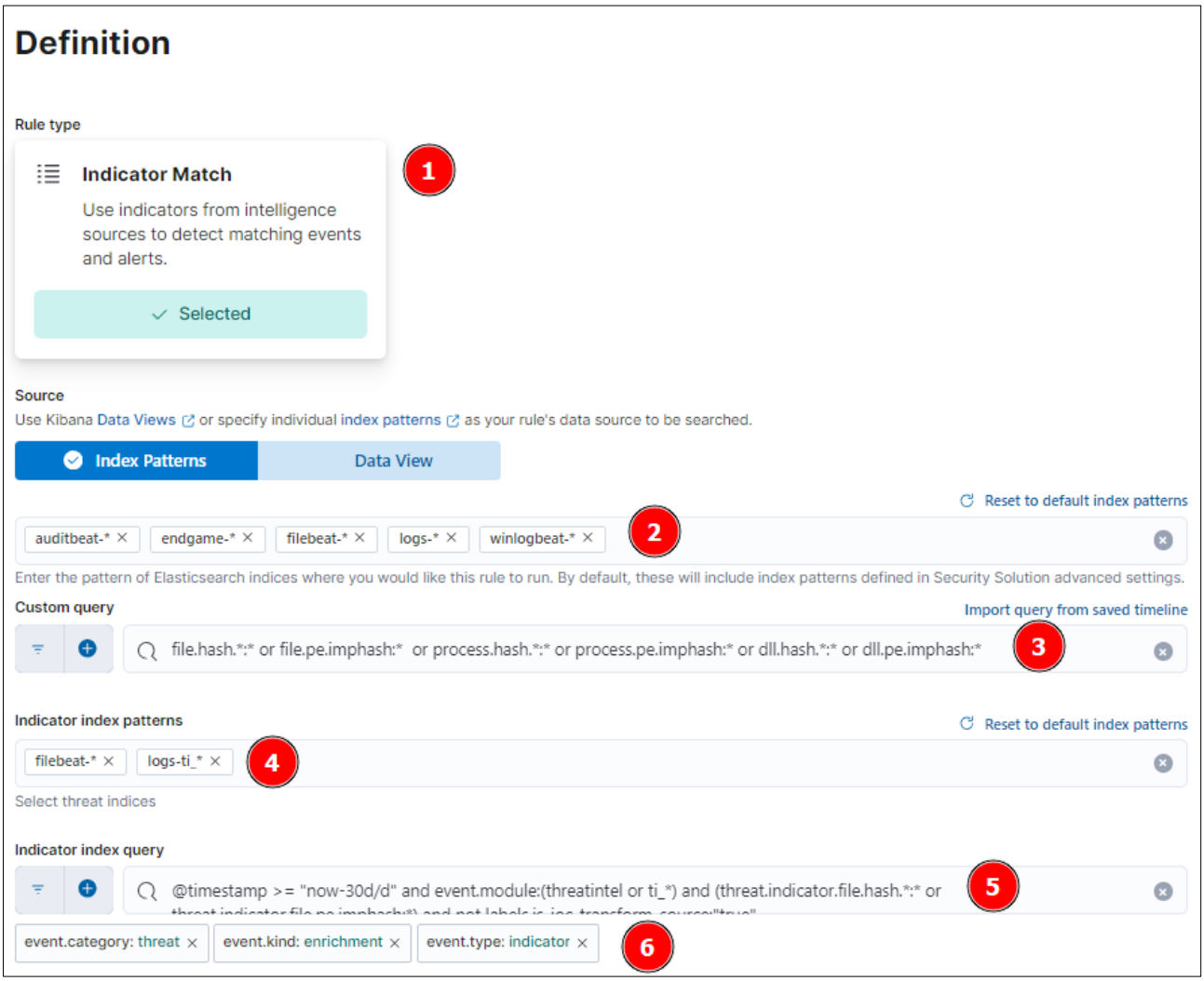


Рисунок 3.20 – Правило, що стосується виявлення збігів хешу

Останнім кроком при створенні правила було зробити маппінг відповідних полей (Рис. 3.21).

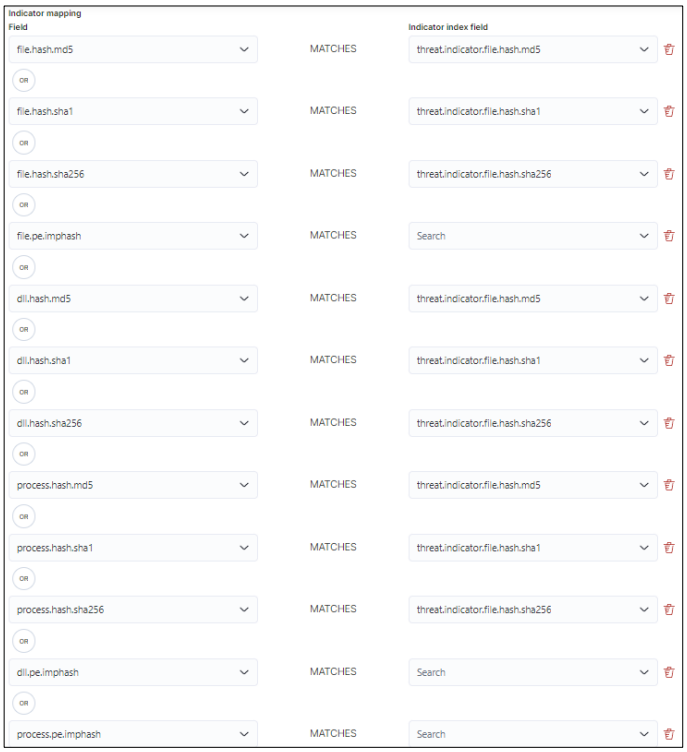


Рисунок 3.20 – Маппінг полей

Для того, щоб перевірити працездатність правила та коректність його відпрацювання, на платформі MISP було створено тестову подію, в якій в якості «індикаторів компрометації» були завантажені легітимні метрики, такі як хеш postgres.exe (Рис 3.21, 3.22).

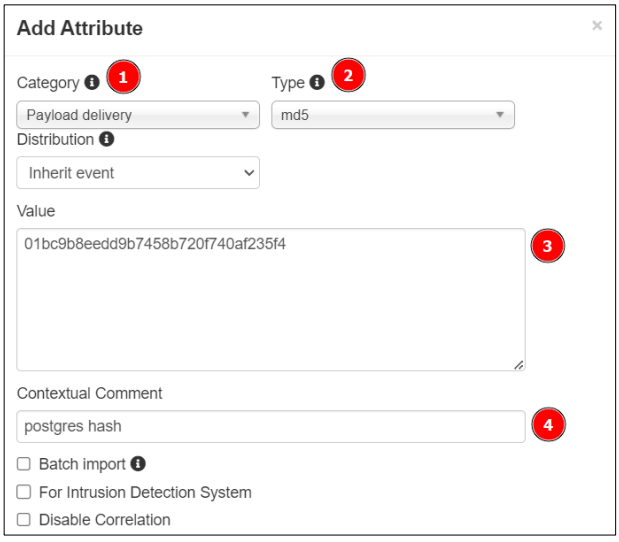


Рисунок 3.21 – Створення тестового індикатору

Рисунок 3.22 – Тестові індикатори

Хеш postgres.exe є в топі хешів у цього замовника, тому відповідний контроль спрацював (Рис. 3.23) майже одразу після того, як індикатор було додано в MISP і як ці дані завантажились в Elastic.

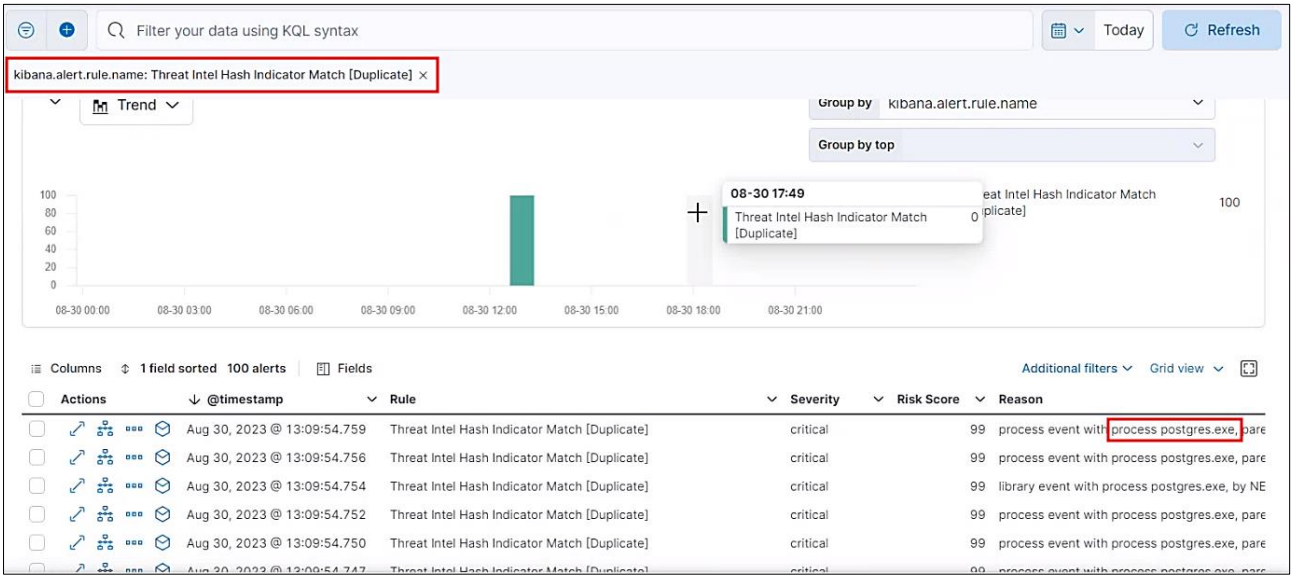


Рисунок 3.23 – Спрацювання створеного правила

Впровадження цієї інтеграції допоможе аналітикам швидше та якісніше дізнаватися про загрози у світі кібербезпеки і реагувати на них.

ВИСНОВКИ

В результаті виконання були розроблені рішення, які допоможуть підвищити ефективність SOC на прикладі обраної організації. Було розглянуто різноманітні підходи до оцінки ефективності та визначено оптимальні з них. Також було надано рекомендацій по підвищенню ефективності, в якості основних з яких були визначені такі дії, як: автоматизація процесів і процедур; розробка плейбуків; підвищення кваліфікації персоналу; впровадження нових інтеграцій; інвестування в технології; регулярні проведення оцінки ефективності.

У ході виконання кваліфікаційної роботи було виконано такі завдання:

1. Проведено аналітичний огляд основних принципів функціонування SOC та його інформаційних технологій.
2. Розглянуто питання організації людських та технічних ресурсів.
3. Визначено критерії оцінки ефективності SOC та проведено її вимірювання (а саме: збір даних про діяльність SOC, аналіз цих даних, оцінка ефективності SOC за розробленими показниками).
4. Надано рекомендації по підвищенню ефективності функціонування SOC.
5. Виконано розробку кількох інструментів для покращення ефективності SOC (а саме написання плейбуку для автоматичної обробки спрацювань, та інтеграція MISP з Elastic).
6. Проведено практичну реалізацію цих рішень та перевірено їх працездатність на практиці.

За результатами роботи впроваджених рішень можна зробити висновок, що їх застосування підвищить якість роботи аналітиків та скоротить час на опрацювання інцидентів.

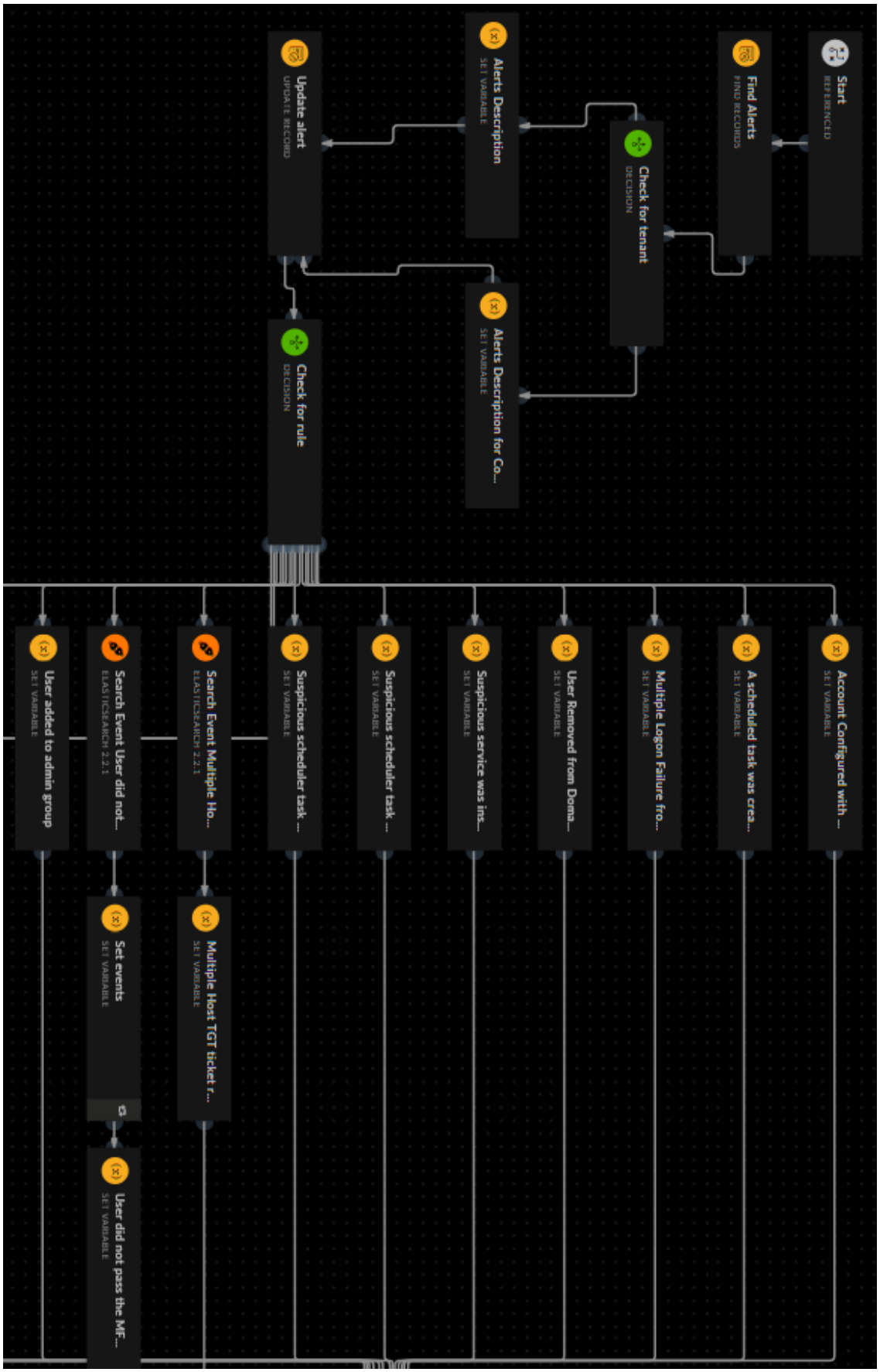
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

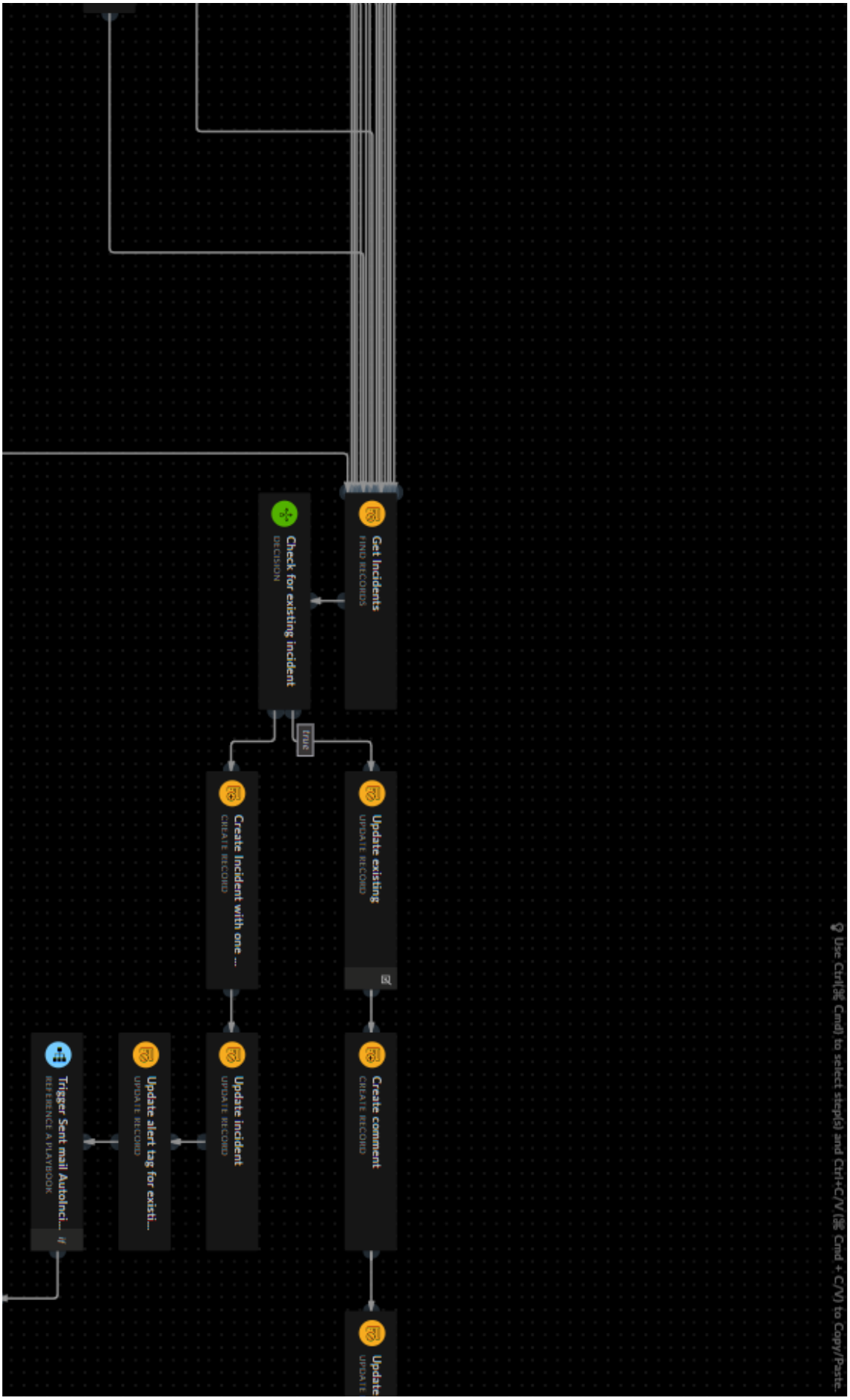
1. What Is a Security Operations Center (SOC)? | Trellix. *Trellix | Revolutionary Threat Detection and Response*. URL: https://www.trellix.com/security-awareness/operations/what-is-soc/ (date of access: 05.10.2023).
2. OpenText. *OpenText*. URL: https://www.opentext.com/what-is/security-operations-center (date of access: 05.10.2023).
3. What is a security operations center (SOC)? *Microsoft*. URL: https://www.microsoft.com/en-us/security/business/security-101/what-is-a-security-operations-center-soc (date of access: 05.10.2023).
4. What is Security Operations Center (SOC)? | IBM. *IBM in Deutschland, Österreich und der Schweiz | IBM*. URL: https://www.ibm.com/topics/security-operations-center (date of access: 05.10.2023).
5. Top security orchestration and response (SOAR) software. *Fortinet*. URL: https://www.fortinet.com/products/fortisoar (date of access: 05.10.2023).
6. SIEM & security analytics | elastic security. *Elastic*. URL: https://www.elastic.co/security/siem (date of access: 05.10.2023).
7. What is EDR? - endpoint detection and response. *Cisco*. URL: https://www.cisco.com/c/en/us/products/security/endpoint-security/what-is-endpoint-detection-response-edr-medr.html (date of access: 06.10.2023).
8. What is EDR (endpoint protection and response)? | IBM. *IBM in Deutschland, Österreich und der Schweiz | IBM*. URL: https://www.ibm.com/topics/edr (date of access: 06.10.2023).
9. What Is Network Detection and Response - NDR. *Cisco*. URL: https://www.cisco.com/c/en/us/products/security/what-is-network-detection-response.html (date of access: 06.10.2023).
10. What is a secure email gateway (SEG)? | Cloudflare. *Cloudflare*. URL: https://www.cloudflare.com/learning/email-security/secure-email-gateway-seg/ (date of access: 06.10.2023).

11. What is a secure email gateway? Definition & Examples | Darktrace. *Darktrace | Cyber security that learns you*. URL: https://darktrace.com/cyber-ai-glossary/secure-email-gateway-seg (date of access: 06.10.2023).
12. What is Deception Technology? Defined & Explained | Fortinet. *Fortinet*. URL: https://www.fortinet.com/resources/cyberglossary/what-is-deception-technology (date of access: 06.10.2023).
13. What Is DNS Protection?. *Imperva*. URL: https://www.imperva.com/learn/application-security/dns-protection/ (date of access: 07.10.2023).
14. Рішення / ІБ / NGFW. *Softlist - смарт рішення у сфері інформаційної безпеки та IT*. URL: https://softlist.ua/servises/ngfw (дата звернення: 07.10.2023).
15. What is user activity monitoring (UAM). *ActivTrak*. URL: https://www.activtrak.com/user-activity-monitoring/ (date of access: 07.10.2023).
16. What is User Activity Monitoring? How It Works, Benefits, Best Practices, and More. *Digital Guardian*. URL: https://www.digitalguardian.com/blog/what-user-activity-monitoring-how-it-works-benefits-best-practices-and-more (date of access: 07.10.2023).
17. Privileged Access Management (PAM) - контроль привілейованих користувачів. *Softprom – IT Distributor | Cyber Security, Cloud, IT Systems, CCTV, CAD*. URL: https://softprom.com/ua/vendor/cyberark/product/privileged-access-management-pam-kontrol-privileyovanih-koristuvachiv (дата звернення: 07.10.2023).
18. Що таке Privileged Access Management (PAM)? *Microsoft*. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-privileged-access-management-pam (date of access: 07.10.2023).

19. Multi-Factor authentication. *Electronic Signature, Cloud Authentication, Mobile App Security | OneSpan*. URL: https://www.onespan.com/topics/multi-factor-authentication (date of access: 07.10.2023).
20. Yasar K., Shacklett M. E. What is Multifactor Authentication? | Definition from TechTarget. *Security*. URL: https://www.techtarget.com/searchsecurity/definition/multifactor-authentication-MFA (date of access: 07.10.2023).

ДОДАТОК А


Start
REFERENCED
Find Alerts
FIND RECORDS
Check for tenant
DECISION
Alerts Description
SET VARIABLE
Update alert
UPDATE RECORD
Alerts Description for Co...
SET VARIABLE
Check for rule
DECISION
Account Configured with ...
SET VARIABLE
A scheduled task was crea...
SET VARIABLE
Multiple Logon Failure fro...
SET VARIABLE
User Removed from Doma...
SET VARIABLE
Suspicious service was inst...
SET VARIABLE
Suspicious scheduler task ...
SET VARIABLE
Suspicious scheduler task ...
SET VARIABLE
Search Event Multiple Ho...
ELASTICSEARCH 2.2.1
Multiple Host TGT ticket r...
SET VARIABLE
Search Event User did not...
ELASTICSEARCH 2.2.1
Set events
SET VARIABLE
User did not pass the MF...
SET VARIABLE
User added to admin group
SET VARIABLE


Use Ctrl(⌘ Cmd) to select step(s) and Ctrl+C/V(⌘ Cmd + C/V) to Copy/Paste.
Get Incidents
FIND RECORDS
Check for existing incident
DECISION
true
Update existing
UPDATE RECORD
Create Incident with one ...
CREATE RECORD
Create comment
CREATE RECORD
Update incident
UPDATE RECORD
Update alert tag for existi...
UPDATE RECORD
Trigger Sent mail AutoInci...
REFERENCE A PLAYBOOK