ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОРПОРАТИВНОЇ МЕРЕЖІ НА ОСНОВІ РІШЕННЯ CISCO SECUREX»

Виконав: студент 6 курсу, групи БСДМ-63
Спеціальності 125 Кібербезпека
Освітньо-професійної програми
«Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Бовкун В.Б.
(прізвище та ініціали)

Керівник Довженко Н.М.
(прізвище та ініціали)

Рецензент _____
(прізвище та ініціали)

Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2022

ВСТУП

Актуальність дослідження. Щоб відповісти на зростаючі потреби безпеки сучасних корпоративних мереж в світі активно створюються різні технології та архітектури. Саме вони мають елементи забезпечення безпеки у вигляді пристроїв, модулів або хмарних служб, побудованих поверх один одного. Новітні архітектури можуть працювати з повним спектром пристроїв, починаючи від традиційних корпоративних ПК або Mac і закінчуючи мобільними пристроями нового покоління, такими як iPad і Android.

Традиційні підходи до безпеки мережі використовували чітко визначені межі для захисту внутрішніх мереж від зовнішніх загроз і зловмисного програмного забезпечення. Співробітники використовували корпоративні комп'ютери, захищені антивірусом та особистими брандмауерами. Мережі на основі периметра були захищені за допомогою пристроїв мережевого сканування (брандмауери, веб-проксі та шлюзи електронної пошти).

Сьогодні мережеві кордони зникають, оскільки користувачі хочуть отримати доступ до ресурсів з будь-якого місця, на будь-якому типі кінцевого пристрою, використовуючи різні методи підключення. Cisco вирішила це за допомогою мережевої архітектури без кордонів, яка об'єднує такі компоненти, як кінцева зона без кордонів, безмежний Інтернет, центр обробки даних без кордонів та надання різних рівнів управління політикою безпеки.

Архітектурний підхід до безпеки, який міститься в безмежній мережевій архітектурі, призводить до створення різних категорій продуктів, технологій і рішень Cisco, одним з таких рішень і стала контекстно-залежна архітектура SecureX, яка забезпечує виконання політик безпеки по всій розподіленій мережі, а не лише в одній точці потоку даних.

Платформа SecureX має на меті поєднати широкий спектр інтегрованого портфоліо безпеки Cisco та інфраструктуру клієнта для злагодженої роботи, яка

уніфікує видимість всіх процесів, забезпечує автоматизацію та зміцнює безпеку в мережі, кінцевій точці, хмарі та програмах.

Об'єкт дослідження – забезпечення інформаційної безпеки корпоративної мережі

Предмет дослідження – технології забезпечення безпеки корпоративної мережі на основі продукту Cisco SecureX.

Мета роботи – розроблення рекомендацій щодо покрокового налаштування рішення Cisco SecureX для забезпечення безпеки корпоративної мережі.

Наукові завдання:

- визначення проблематики інформаційного захисту корпоративних мереж;
- дослідити чинні загрози та вразливості корпоративних мереж;
- дослідити принципи роботи, функціональні особливості продукту Cisco SecureX та інтегрувати його в роботу корпоративної мережі.

Практичне значення одержаних результатів: дослідження роботи продукту та рекомендації щодо захисту можуть бути використані у сфері забезпечення кібербезпеки у корпоративних мережах.

1 АНАЛІЗ СУЧАСНОГО СТАНУ ЗАХИСТУ ДАНИХ В КОРПОРАТИВНИХ МЕРЕЖАХ

1.1. Категорії загроз безпеки корпоративних мереж

Корпоративна мережа є великою, складною та, ймовірно, покладається на численні підключені кінцеві точки. Незважаючи на те, що це корисно для бізнес-операцій і спрощує підтримку робочого процесу, це також становить проблему для безпеки. Проблема в тому, що легкість пересування означає, що якщо зловмисник отримує доступ до мережі, він може вільно пересуватися та завдавати шкоди, часто без відома співробітників компанії. Ці загрози мережевій безпеці роблять організацію дуже вразливою до витоку даних [1].

Мережева атака — це спроба отримати неавторизований доступ до мережі організації з метою викрадення даних або виконання інших шкідливих дій. Існує два основних типи мережевих атак:

- Пасивний: зловмисники отримують доступ до мережі та можуть контролювати або викрадати конфіденційну інформацію, але не змінюючи дані, залишаючи їх недоторканими.
- Активний: зловмисники не лише отримують неавторизований доступ, але й змінюють дані, видаляючи, шифруючи чи іншим чином пошкоджуючи їх.

Зловмисник, що отримав доступ в мережу, відразу стає джерелом чотирьох видів загроз [2]:

1. Отримання несанкціонованого доступу до конфіденційних даних;
2. Отримання несанкціонованого доступу до керування робото ІС;
3. Знищення або спотворення даних;
4. Порушення або повне припинення роботи ІС.

Рис. 1.1. Види загроз інформаційній безпеці корпоративної мережі

Отримання несанкціонованого доступу - проникнення в комп'ютер для отримання конфіденційної інформації. Ця інформація може бути використана або продана з різними цілями. Приклад: розкрадання конфіденційної інформації, що належить організації, наприклад, відомості про науковотехнічні розробки. Використовуючи ці дані, людина може отримати юридичні документи, подати заяву на кредит та здійснити несанкціоновані покупки через Інтернет. Проблема крадіжки особистої інформації продовжує загострюватися, а фінансові втрати становлять мільярди доларів на рік.

Знищення або спотворення даних - проникнення в комп'ютер з метою знищення або зміни записів даних. Приклади втрати даних: передача вірусу, що затирає жорсткий диск комп'ютера. Приклад неправомірного використання даних: проникнення в систему зберігання даних з метою зміни даних, наприклад ціни виробу.

Порушення або повне припинення роботи ІС - заборона доступу правомірних користувачів до служб, для використання яких, їм має бути надане право. Приклад: атаки типу «відмова в обслуговуванні» (DoS-атаки) на сервери, мережеві пристрої і канали обміну даними по мережі [2].

Таким чином, навіть у невеликих мережах необхідно враховувати загрози безпеці та вразливості при плануванні впровадження мережі

1.2. Вектори втрат даних

Втрата даних є серйозною незручністю, яка порушує повсякденну роботу будь-якого інформаційного бізнесу. Коли важливі файли та документи втрачаються, організація повинна витрачати час і ресурси на відтворення або відновлення цих файлів, щоб заповнити прогалини, утворені втратою. Втрата даних, спричинена пошкодженням або вірусами, створює особливі проблеми, оскільки інколи буває важко визначити ступінь спричиненої шкоди. Відновлювати пошкоджені файли може бути дорого для компанії.

Втрата даних також сповільнює терміни продуктивності та може призвести до втрати клієнтів, якщо це супроводжується порушеннями безпеки. Якщо конфіденційні дані викрадено або пошкодженно, компанія повинна розкрити це клієнтам, що призведе до втрати довіри та поваги. Навіть якщо компанія зможе відновити втрату даних, згодом доведеться витратити час на відновлення відносин з клієнтами.

Незручність втрати даних може мати ще більші наслідки для бізнесу, якщо втрачено великий обсяг даних [3]:

- 94 відсотки компаній, які зазнали серйозної втрати даних, не відновлюються;
- 51 відсоток цих компаній закриваються протягом двох років після втрати даних;
- 43 відсотки цих компаній більше не відкриваються;
- 70 відсотків малих фірм припиняють роботу протягом року після великої втрати даних;

Залишати дані незахищеними — дорогий ризик — середня вартість витоку даних для американської компанії, згідно з дослідженням IBM , становила 8,6 мільйона доларів — найвищий показник у світі. Те саме дослідження показало,

що для виявлення та локалізації витоку даних може знадобитися 280 днів – більше дев’яти місяців.

Втрата даних може бути викликана багатьма різними факторами, і кожен створює унікальну проблему для відновлення даних. Збої жорсткого диска спричиняють найвищий відсоток втрати даних, але людські помилки та проблеми з програмним забезпеченням йдуть слідом за ними.

Згідно з даними Kroll Ontrack:

- 67 відсотків втрат даних викликано збоями жорсткого диска або системними збоями;
- 14 відсотків втрат даних викликано людською помилкою;
- 10 відсотків втрати даних є результатом програмного збою;

Обізнаність про вектори втрати даних і ризики, пов’язані з втратою даних, має важливе значення для запобігання втраті даних, яка може стати великими витратами для бізнесу:

- людська помилка;
- віруси та шкідливі програми;
- пошкодження жорсткого диска;
- відключення електроенергії;
- комп'ютерна крадіжка;
- пошкодження рідиною;
- катастрофи;
- пошкодження програмного забезпечення;
- форматування жорсткого диска;
- хакери та інсайдери.

1.Людська помилка. Люди не непогрішні — всі роблять помилки, і іноді вони великі. Для компаній ці помилки можуть призвести до ненавмисного видалення файлів даних або фрагментів тексту. Самі того не усвідомлюючи, співробітники можуть перезаписати важливі файли або видалити інформацію, важливу для бізнесу. Людська помилка також може зіграти роль у багатьох інших

основних причинах втрати даних, включаючи пошкодження жорсткого диска, розлиття рідини, пошкодження програмного забезпечення та форматування жорсткого диска.

Одним із важливих заходів для запобігання людським помилкам під час обробки даних є належне навчання. Необхідно переконатися, що співробітники розуміють, як працює обробка даних у компанії та як функціонують системи резервного копіювання. Це може бути так само просто, як дізнатися, чи документи, з якими вони працюють, автоматично створюватимуться у резервні копії, чи вони повинні вручну зберігати файли під час роботи.

Помилки, спричинені помилками людини, також можна мінімізувати за допомогою кількох програмних засобів. Автоматизація мінімізує кількість взаємодії людини з даними, що знижує ризик видалення або перезапису. Оптимізований робочий процес також залишає мало місця для людських помилок, заощаджуючи час співробітників і полегшуючи виявлення помилок. Системи резервного копіювання також слід використовувати для збереження попереднього стану даних [3].

Відновлення випадково видалених або перезаписаних даних іноді може бути таким же простим, як пошук у кошику комп’ютера. В інших випадках можна отримати доступ до попередньо збережених версій документа. Коли втрачені дані не так легко відновити, програмне забезпечення для відновлення файлів може стати чудовим інструментом. Програмне забезпечення для відновлення файлів сканує жорсткий диск комп’ютера, щоб визначити та відновити втрачені дані.

2. Віруси та шкідливі програми. Більшість людей думають про віруси, коли їх запитують, що спричиняє втрату даних. Для підприємств віруси можуть викрадати та видаляти масиви даних або призводити до призупинення бізнес-операцій, руйнуючи функціональність компанії. Комп’ютер часто отримує вірус під час атаки на основі електронної пошти або через фішинг, який спокушає співробітника натиснути на пошкоджене посилання. Потім це посилання дозволяє вірусу або шкідливому програмному забезпеченню проникнути в комп’ютерну систему, щоб пошкодити або викрасти файли.

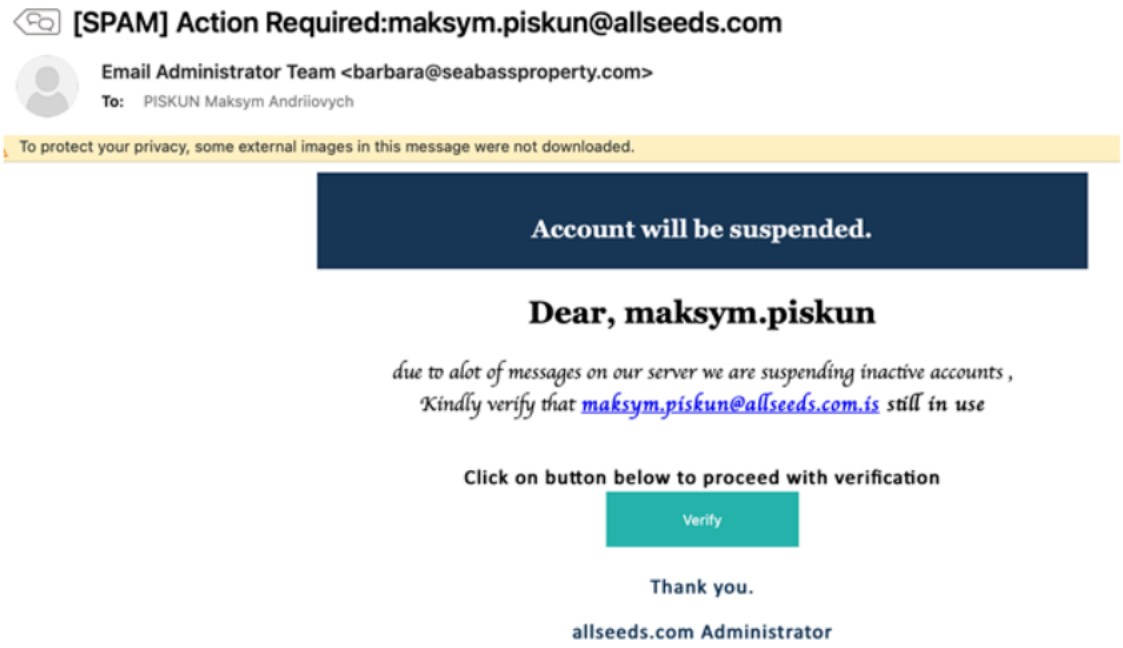

Рис. 1.2. Приклад фішингового посилання

3. Пошкодження жорсткого диска. Більшість втрат даних відбувається через несправності апаратного забезпечення, головним винуватцем яких є жорсткий диск. Жорсткі диски є найбільш крихкими частинами комп'ютерів, і щотижня виходить з ладу близько 140 тисяч жорстких дисків. З цих аварій 60 відсотків спричинені механічними проблемами, а 40 відсотків — результатом неправильного або неправильного поводження з боку людини, зокрема падіння чи штовхання комп'ютера чи ноутбука. Жорсткі диски також можуть бути пошкоджені, якщо комп'ютер перегрівається, як правило, через надмірне використання або накопичення пилу в комп'ютері.

Однак, як і будь-яка інша машина, жорсткий диск з часом зношується і з часом перестає працювати. Нижче наведено кілька ознак, на які слід звернути увагу, які вказують на те, що жорсткий диск може вийти з ладу [4]:

- часто виходить з ладу жорсткий диск;
- комп'ютер надзвичайно гарячий;
- під час завантаження виникають проблеми з жорстким диском;
- швидкість обробки постійно знижується;
- комп'ютер часто зависає;

- комп’ютер видає клацання або скрегіт;
- файли не відкриваються або випадково пошкоджуються.

SSD або твердотільні накопичувачі також з’являються як альтернатива традиційним HDD або жорстким дискам. Накопичувачі SSD не мають рухомих частин, тому вони більш довговічні у використанні, ніж жорсткі диски. Крім того, менша ймовірність несправності або збою в роботі твердотільних накопичувачів, що означає меншу ймовірність втрати даних. Однак комп’ютери з твердотільними накопичувачами також, як правило, дорожчі, ніж комп’ютери зі стандартними жорсткими дисками, і можуть бути фінансово невигідними для кожного підприємства. Вживання профілактичних заходів для захисту даних комп’ютера є важливим незалежно від типу жорсткого диска.

4. Відключення електроенергії. Перебої в електропостачанні можуть суттєво переривати бізнес-операції, вимикаючи програмні системи без попередження. Це може призвести не лише до втрати незбережених даних, але й до пошкодження існуючих файлів через неправильні процедури завершення роботи. Іноді цілі програми можуть стати нефункціональними через невчасне відключення електроенергії. Якщо комп’ютер вимикається під час запису на жорсткий диск, він може більше ніколи не запуститися [5].

Навіть якщо не втратяться дані під час відключення електроенергії, неправильне завершення роботи може мати тривалий вплив на жорсткі диски комп’ютера. Якщо часті перебої або перепади електроенергії відбуваються, термін служби жорсткого диска значно скорочується, а ймовірність його збою зростає.

Найкращий спосіб захисту від цих проблем — регулярне автоматичне резервне копіювання системи. Резервне копіювання часто є єдиним способом відновити втрачені дані після відключення електроенергії. Бізнес також повинен використовувати пристрої захисту від перенапруг, щоб запобігти можливому пошкодженню через стрибки напруги. Наявність генератора або резервної акумуляторної системи також може дозволитивам зберегти або створити резервну копію бізнес-даних під час відключення електроенергії.

5. Крадіжка комп'ютера або ноутбука. На сучасному робочому місці все більше людей стають мобільними. Це часто означає, що вони працюють з ноутбуків або смартфонів, а не з ПК. Крадіжка ноутбука є серйозним ризиком і може статися будь-де, якщо ноутбук залишити без нагляду. Згідно з дослідженням:

- 25 відсотків крадіжок IT відбувається в автомобілях або інших транспортних засобах;
- 23 відсотки займає місце в офісі;
- 15 відсотків відбувається в аеропортах або готелях;
- 12 відсотків відбувається в ресторанах.

Окрім втрати даних, крадіжка ноутбука також створює загрозу витоку даних. Якщо співробітники компанії зберігають або отримують доступ до конфіденційної інформації на портативних пристроях, необхідно мати засіб дистанційного видалення даних із цих ноутбуків або планшетів. Необхідно переконатися, що важливі дані, які зберігаються на ноутбуках, створені в безпечному місці [6].

Необхідно переконатися, що комп’ютери в офісній будівлі зберігаються в закритих приміщеннях, доступ до яких мають лише працівники, уповноважені ними користуватися.

Якщо у компанії використовуються ноутбуки, які містять цінну інформацію, слід розглянути можливість встановлення на ці пристрої Це програмне забезпечення дозволяє відстежувати вкрадений ноутбук, щоб правоохоронні органи змогли повернути викрадений пристрій. Програмне забезпечення для захисту від крадіжок часто містить опцію дистанційного стирання, якщо на ноутбуці зберігаються цінні дані.

6. Пошкодження рідиною. Проливання кави або води на ноутбук або комп’ютер може спричинити коротке замикання, що ускладнить відновлення комп’ютера, не кажучи вже про дані, що зберігаються в ньому. Якщо комп’ютер якимось чином повністю занурюється під воду, ситуація стає ще серйознішою. Іноді може здаватися, що комп’ютер працює добре після розливу, але внутрішнє

пошкодження може мати тривалі наслідки, які призведуть до короткого замикання комп’ютера в майбутньому. Кислі напої, такі як кава, становлять особливу небезпеку, оскільки вони можуть роз’їсти внутрішню частину комп’ютера, якщо розлиту речовину не прибрати належним чином.

7. Катастрофи. Від торнадо до пожежі, лиха можуть статися тоді, коли найменше їх очікують, і мати руйнівний вплив на бізнес. Вони можуть знищити ваш комп’ютер, ваші дані і навіть повністю ваш бізнес. Щоб мінімізувати наслідки стихійного лиха та забезпечити продовження, створюйте резервні копії даних щотижня та зберігайте файли в безпечному місці.

Стихійні лиха можуть завдати непоправної шкоди бізнесу, якщо дані не резервуються [2]:

- 93 відсотки компаній, які втратили центр обробки даних на 10 або більше днів через катастрофу, подали заяви про банкрутство протягом одного року;
- 50 відсотків компаній, які втратили керування даними через катастрофу, негайно оголосили про банкрутство;
- 30 відсотків підприємств, які зазнали серйозної пожежі, припиняють роботу протягом року;
- 70 відсотків підприємств, які зазнали серйозної пожежі, припиняють роботу протягом п’яти років.

Оскільки стихійні лиха можуть повністю зруйнувати технологію компанії, часто неможливо відновити дані, втрачені через катастрофу. Ось чому так важливо створювати резервні копії даних у віддаленому місці, яке не може бути скомпрометовано місцевою катастрофою.

8. Пошкодження програмного забезпечення. Несподіване або неправильне завершення роботи програмного забезпечення може здатися невинним на перший погляд, але може спричинити серйозні проблеми з вашими даними. Неправильне завершення роботи може пошкодити ваші дані або видалити прогрес, втрачаючи час і цінні дані. Якщо програмне забезпечення пошкоджено, воно може не

працювати знову, тобто не буде змоги отримати доступ до даних, які зберігаються в цьому програмному забезпеченні.

Хоча пошкодження програмного забезпечення іноді може бути наслідком відключення електроенергії або інших неконтрольованих факторів, важливо впроваджувати процедури належного завершення роботи програмного забезпечення після кожного використання.

9. Форматування жорсткого диска. Випадкове форматування жорсткого диска може призвести до миттєвої втрати даних. Співробітники можуть випадково відформатувати жорсткий диск, якщо неправильно зрозуміють системні підказки чи повідомлення про помилки. Переформатування також може статися під час оновлення системи та призвести до втрати даних. Хоча випадкове переформатування жорсткого диска може призвести до паніки, коли більше немає доступу до файлів і документів, часто можна відновити втрачені дані під час форматування жорсткого диска, запустивши програмне забезпечення для відновлення даних.

10. Хакери та інсайдери. Останніми роками хакерство та витік даних стали набагато більш поширеною проблемою, що робить необхідні заходи для кібербезпеки. Неавторизовані гості у мережі можуть завдати серйозної шкоди вашим даним, видаливши та викравши будь-які дані, які вони бажають. Вони можуть навіть пошкодити цілі мережеві процеси, якщо мають достатній доступ до системи.

Хакери можуть отримати доступ до даних різними способами. Ось кілька речей, яких слід уникати, щоб система не була вразливою для хакерів [3]:

- використання серверів із низьким рівнем безпеки;
- відсутність відповідних брандмауерів;
- використання паролів, які легко вгадати.

Сумна правда полягає в тому, що дані іноді викрадають або скомпрометовують самі працівники чи інші особи. У багатьох випадках дані, викрадені хакерами або інсайдерами, неможливо відновити. Важливо вживати заходів для запобігання кібератакам і часто створювати резервні копії даних.

1.3. Класифікація атак на корпоративні мережі

Існує декіла видів мережевих атак:

- Атаки на кінцеві точки — отримання несанкціонованого доступу до пристроїв користувачів, серверів або інших кінцевих точок, зазвичай під загрозою їх зараження шкідливим програмним забезпеченням [12].
- Атаки зловмисного програмного забезпечення — зараження IT-ресурсів шкідливим програмним забезпеченням, що дозволяє зловмисникам скомпрометувати системи, викрасти дані та завдати шкоди. Сюди також входять атаки програм-вимагачів [8].
- Уразливості та експлойти — використання вразливостей у програмному забезпеченні, що використовується в організації, для отримання несанкціонованого доступу, компрометації чи саботажу систем.
- Розширені стійкі загрози — це складні багаторівневі загрози, які включають мережеві атаки, а також інші типи атак.

Під час мережевої атаки зловмисники зосереджені на проникненні в периметр корпоративної мережі та отриманні доступу до внутрішніх систем. Дуже часто, потрапивши всередину, зловмисники комбінують інші типи атак, наприклад, компрометуючи кінцеву точку, розповсюджуючи зловмисне програмне забезпечення або використовуючи вразливість у системі в мережі.

Нижче наведено поширені вектори загроз, які зловмисники можуть використовувати для проникнення у мережу:

1. Неавторизований доступ. Неавторизований доступ стосується доступу зловмисників до мережі без отримання дозволу. Серед причин атак несанкціонованого доступу – слабкі паролі, відсутність захисту від соціальної інженерії, раніше зламані облікові записи та внутрішні загрози [10].

2. Атаки розподіленої відмови в обслуговуванні (DDoS) Зловмисники створюють ботнети, великі групи скомпрометованих пристроїв і використовують їх для спрямування помилкового трафіку у вашу мережу або сервери. DDoS може відбуватися на рівні мережі, наприклад, шляхом надсилання

величезних обсягів пакетів SYN/ACC, які можуть перевантажити сервер, або на рівні програми, наприклад, шляхом виконання складних запитів SQL, порушуючи роботу бази даних [9].

3. Атака «людина посередині» передбачає перехоплення зловмисниками трафіку між мережею та зовнішніми сайтами або всередині вашої мережі. Якщо протоколи зв'язку не захищені або зловмисники знаходять спосіб обійти цей захист, вони можуть викрасти дані, що передаються, отримати облікові дані користувача та захопити їхні сесії [10].

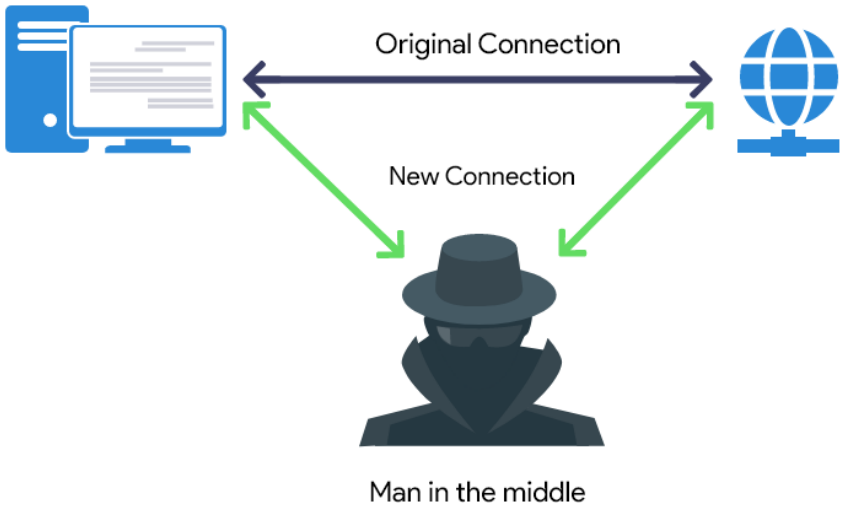

Рис. 1.3. Атака «людина посередині»

4. Атаки з впровадженням коду та SQL. Багато веб-сайтів приймають введені користувачем дані та не перевіряють та не очищають їх. Потім зловмисники можуть заповнити форму або здійснити виклик API, передаючи зловмисний код замість очікуваних значень даних. Код виконується на сервері та дозволяє зловмисникам скомпрометувати його.

5. Ескалація привілеїв. Як тільки зловмисники проникають у мережу, вони можуть використовувати ескалацію привілеїв для розширення свого охоплення. Горизонтальна ескалація привілеїв передбачає отримання зловмисниками доступу до додаткових, суміжних систем, а вертикальна ескалація означає, що зловмисники отримують більш високий рівень привілеїв для тих самих систем.

6. Внутрішні загрози. Мережа особливо вразлива для зловмисних інсайдерів, які вже мають привілейований доступ до систем організації. Інсайдерські загрози може бути важко виявити та захиститися від них, оскільки інсайдерам не потрібно проникати в мережу, щоб завдати шкоди. Нові технології, такі як User and Even Behavioral Analytics (UEBA), можуть допомогти виявити підозрілу або аномальну поведінку внутрішніх користувачів, що може допомогти виявити інсайдерські атаки.

Висновки до першого розділу

Проаналізовано чотири категорії загроз безпеки коропративній мережі. Зазначено що мережеві атаки мають декілька видів отримати неавторизований доступ – пасивний та активний.

Наведено основні вектори втрат даних, що можуть спричинити порушення продуктивності роботи бізнес-процесів або їх повну зупинку.

Вивчено та надано класифікацію атак, що можуть бути здійснені на корпоративну мережу, надано базові рекомендації щодо їх попередження та усунення.

ДОСЛІДЖЕННЯ РІШЕННЯ CISCO SECUREX У ЯКОСТІ МЕХАНІЗМУ ЗАБЕЗПЕЧЕННЯ ТА КОНРОЛЮ БЕЗПЕКИ КОРПОРАТИВНИХ МЕРЕЖ

2.1. Дослідження ринку використання рішення Cisco Securex та його переваги

2.1.1. Переваги використання рішеннння Cisco Securex

SecureX — це хмарна вбудована платформа в рамках глобального рішення Cisco Secure, підключена до інфраструктури компанії, яка інтегрована та відкрита для простоти роботи. Об’єднує численні різнорідні датчики та технології виявлення порушень та вторгнень безпеки корпоративної мережі, а також забезпечує можливості оркестровки - автоматизація рутинних завданнь за допомогою попередньо створених робочих процесів, які відповідають поширеним сценаріям використання, для максимізації операційної ефективності для захисту мережі, користувачів і кінцевих точок, хмари та програм.

Завдяки SecureX служби безпеки можуть [11]:

● Радикально скоротити час очікування та виконання завдань, якими займається працівник, пов’язані із виявленням, дослідженням і усуненням загроз для протидії атакам або забезпеченням доступу та керування політикою.

● Заощаджувати час і покращувати співпрацю, пов’язану з оркеструванням і автоматизацією безпеки між командами SecOps, ITOps і NetOps, що допомагає підвищити рівень безпеки за допомогою наявних ресурсів і досягти більш бажаних результатів за допомогою вимірюваних, значущих показників.

● Пришвидшити оцінку ефективності та скоротити витрати з реальними перевагами за 15 хвилин – навіть якщо починається з малого, створюючи один продукт, який з часом розвивається відповідно до потреб, щоб консолідувати постачальників та засоби безпеки без шкоди для ефективності безпеки.

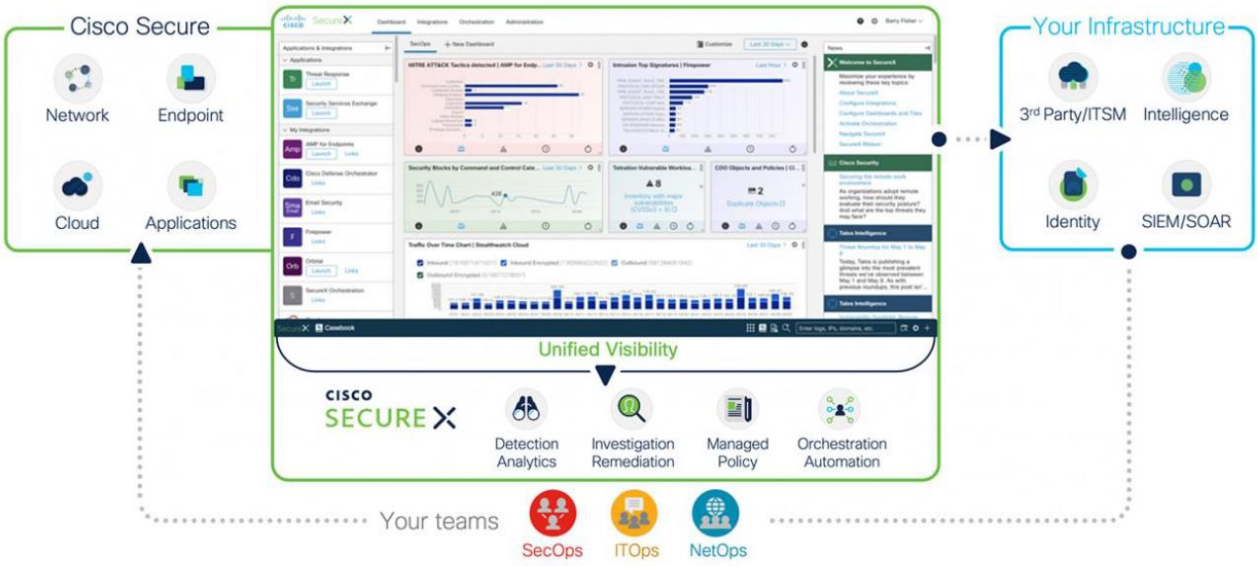

Рис. 2.1. Об'єднані програми в рамках системи SecureX

Основні запити клієнтів по роботі з рішенням Cisco SecureX:

- Пріоритезація інцидентів. Пріоритезація найбільш критичних ситуацій з показниками та оперативними заходами для продуктів і орієнтація на деталізацію продукту.

Результат:

1. Швидше розслідування інцедентів.

2. Розслідування актуальних та потрібних речей.

- Виявлення загроз. Завчасний пошук активних загроз в контрольних точках середовищі компанї за допомогою цілісного інтегрованого підходу, щоб побачити повний масштаб ситуації через спільний контекст і керування випадками.

Результат: Більше можливостей знаходити загрози, які вплинули на корпоративну мережу, і можливість реагувати належним чином.

- Реагування на інциденти. Керування наслідками атаки у середовищі корпоративної мережі, об'єднуючи кілька технологій безпеки для спільного контексту та керування справами, щоб провести цілісне розслідування та виправити ситуацію на одній платформі.

Результат:

1. Швидше реагування.
2. Зменшення часу перебування зловмисника в системі та збитку.

- Автоматизовані та організовані робочі процеси. Автоматизування робочих процесів для SecOps, NetOps та ITOps, щоб керувати кінцевою точкою, мережею та хмарною політикою та захистом ефективніше.

Результат:

1. Автоматизовані та організовані робочі процеси.
2. Стратегічне управління безпекою. Усвідомлення загроз, спрямованих на середовище корпоративної мережі.
3. Єдиний погляд на поточний ландшафт безпеки – управління та захист високого рівня – в організації.

2.1.2. Інтеграція продукту Cisco SecureX з іншими рішеннями Cisco Secure

З кожним роком продукт Cisco Secure розширює свої можливості, азом з цим додаються нові інтеграції.

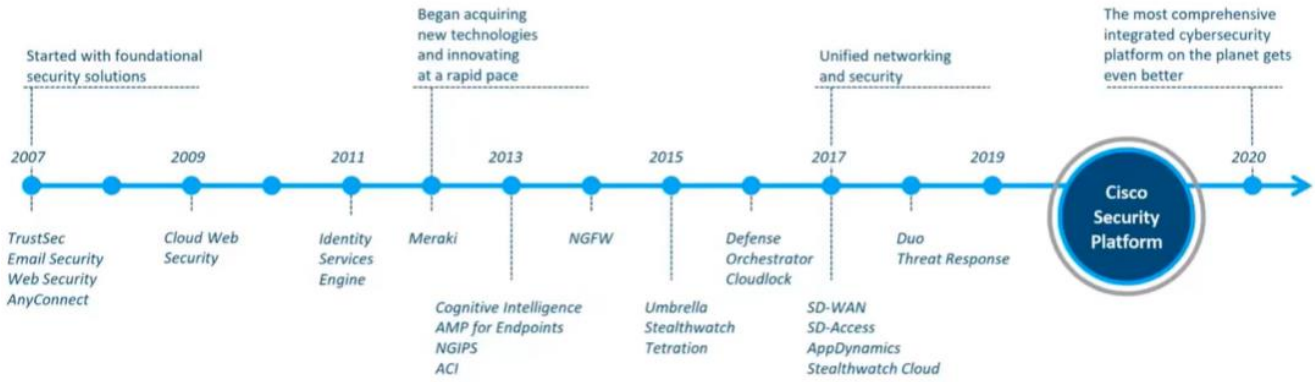

Рис. 2.2. Розвиток платформи

1. SecureX Cisco Secure Endpoint (раніше AMP для кінцевих точок). Secure Endpoint забезпечує захист, керований агентом, керований хмарою, для

фізичних і віртуальних кінцевих систем. У SecureX Secure Endpoint можна використовувати як датчик для визначення наявності зловмисних файлів або мережевих підключень до певних хостів. Його також можна використовувати для застосування звичайних і критичних дій реагування, пов’язаних із кінцевою точкою. SecureX Secure Endpoint надає інформаційні панелі, а також дії для оркестровки, щоб клієнти могли створювати автоматизовані робочі процеси. Крім того, Secure Endpoint містить стрічку SecureX, що дозволяє використовувати функції SecureX з будь-якої сторінки в консолі Secure Endpoint.

Результат [11]:

● Можливість переглядали файли або мережеві ресурси до десятків тисяч глобально розподілених кінцевих точок у вашому середовищі.

● Дистанційне ізолювання потенційно інфікованих хостів у будь-якій точці світу, де є браузер і підключення до Інтернету.

2. Cisco Orbital. Orbital надає глибоко структуровану мову запитів, яка обробляє стан системи як базу даних, дозволяючи проводити детальні перевірки системи в режимі реального часу. Каталог містить набір попередньо створених запитів для виявлення загроз, реагування на інциденти тощо, і користувачі можуть написати власні за допомогою знайомої SQL-подібної структури. У SecureX Orbital є однією зі стрічкових програм, тому до неї можна швидко отримати доступ із консолі будь-якого продукту, що підтримує стрічку. Крім того, вона доступна через зведені модулі, керовані програмою реагування на загрози SecureX.

Результат: За лічені секунди запускаються глибокі та детальні запити про стан системи паралельно для всього розгортання.

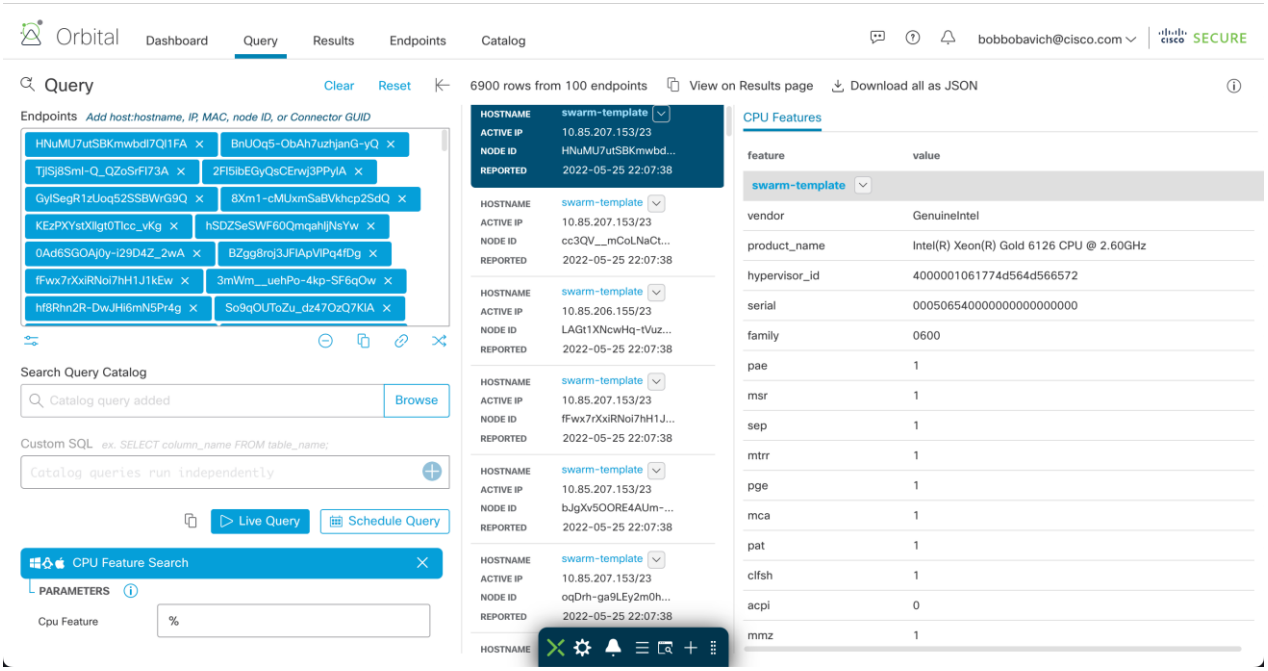

Рис. 2.3. Cisco Orbital

3. Cisco Secure Malware Analytics (раніше Threat Grid). Secure Malware Analytics – це автоматизоване рішення Cisco для перевірки зловмисного програмного забезпечення та аналізу загроз. У SecureX це дозволяє користувачам отримувати детальну інформацію про зловмисне програмне забезпечення, пов'язаний мережевий трафік, системні зміни тощо.

Результат: Покращена інформація про загрози зловмисного програмного забезпечення, отримана за допомогою автоматичного знищення підозрілих файлів із глобальної бази користувачів.

4. Cisco Secure Network Analytics (раніше Stealthwatch) Secure Network Analytics – це рішення для виявлення та реагування мережі (NDR), яке забезпечує безагентну видимість у приватній мережі та загальнодоступній хмарі. У SecureX Secure Network Analytics збагачує виявлення загроз і реагування на них безагентними можливостями виявлення поведінки та відхилень. Інтеграція SecureX з іншими джерелами глобальної інформації про загрози та внутрішньої видимості підтвердить і збагатить висновки Secure Network Analytics підтвердженою інформацією про загрози та локальними спостереженнями [11].

Результат:

● Економія часу і більш цілісне й ефективне реагування, використовуючи SecureX для обробки й керування високопріоритетними сповіщеннями від Secure Network Analytics (та будь-яких інших налаштованих технологій сповіщень).

● Крім того, можливість запитувати всі налаштовані пристрої Secure Network Analytics у відповідь на загрози SecureX, а потім використовувати їх у скоординованому захисті одним клацанням миші, що спрощує видимість і підвищує ефективність реагування.

5. Cisco Secure Cloud Analytics (раніше Stealthwatch Cloud) Secure Cloud Analytics забезпечує аналітику поведінки у корпоративній мережі для кращої видимості, щоб допомогти швидше ідентифікувати складні загрози, від приватної мережі до загальнодоступної хмари [13].

Результат: Прискорення розслідувань завдяки кращій видимості.

6. Cisco Secure Email (раніше Email Security) Secure Email надає можливості захисту від загроз, які швидше виявляють, блокують і усувають загрози у вхідній електронній пошті. У SecureX ця інтеграція дозволяє розуміти електронну пошту як вектор загрози, візуалізуючи зв'язки між повідомленням, відправником і метою в контексті загрози. Можливо одночасно шукати кілька адрес електронної пошти, рядків теми та вкладень, щоб зрозуміти, як поширилася загроза.

Результат: Краще розуміння контексту загрози за допомогою електронної пошти як вектора загрози. Робота з фішинговими атаками, компрометацією корпоративної електронної пошти, шкідливим програмним забезпеченням і програмами-вимагачами.

1. Cisco Umbrella. DNS і хмарна безпека забезпечують захист від доменних загроз у всьому підприємстві, включно з хмарою. У SecureX Umbrella забезпечує:

● Глобальну розвідку про загрози зі своєї багатої бази даних багатогранної репутації домену.

● Відомості про локальну безпеку шляхом звітування про виявлення досліджуваних доменів

● Можливість блокувати домени негайно та на рівні підприємства двома кліками.

Результат: Збагачення всіх розслідувань провідною інформацією про репутацію доменів тощо. Виявлення та швидке блокування джерела атак, одержувачів потенційного чи виявленого витоку даних або інші частини інфраструктури противника.

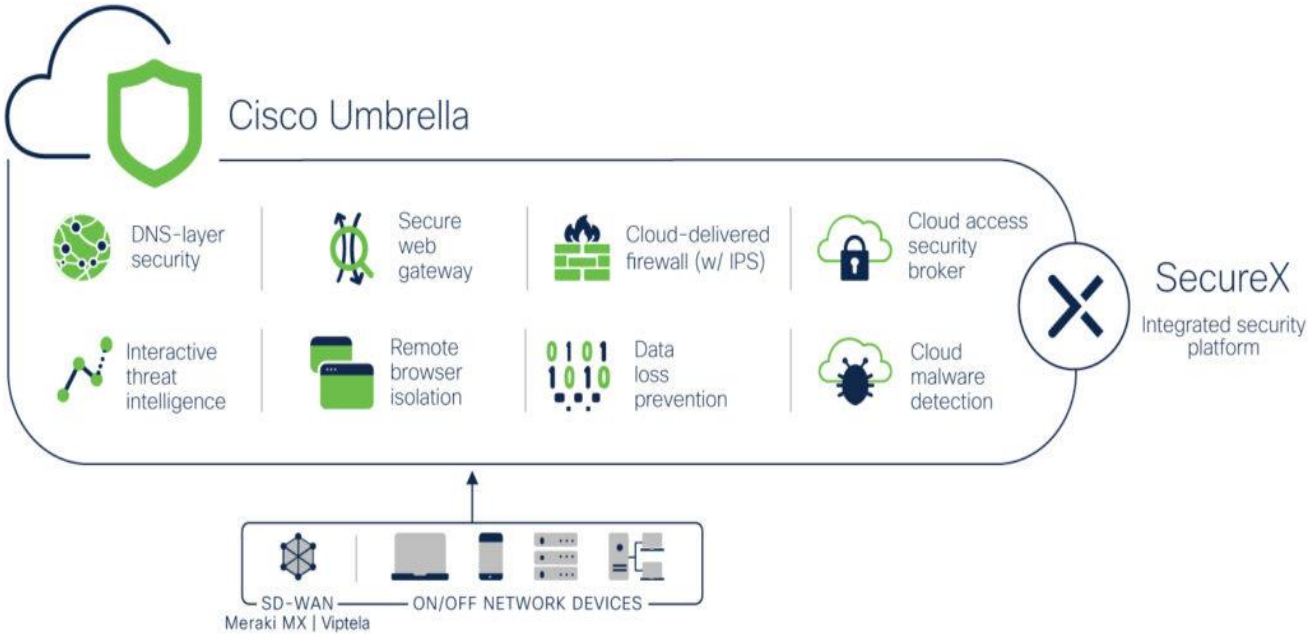

Рис. 2.4. Cisco Umbrella

2. Cisco Secure Firewall. Пристрої Secure Firewall захищають межі корпоративної мережі за допомогою найсучасніших механізмів перевірки пакетів, захисту та запобігання вторгненням, використовуючи розширену систему аналізу загроз TALOS. У SecureX безпечний брандмауер забезпечує спостереження за IP-адресами, URL-адресами та доменом. Крім того, користувачі можуть використовувати пристрої Secure Firewall через SecureX для блокування IP-адрес на периметрі. Нарешті, пристрої Secure Firewall можна налаштувати для надання сповіщень хмарній платформі зберігання подій Cisco для сортування та кореляції таким чином, щоб найактуальніші сповіщення відображалися користувачеві в диспетчері інцидентів SecureX.

Результат:

● Економія часу і більш цілісне й ефективне реагування, використовуючи SecureX для обробки й керування високопріоритетними сповіщеннями від усіх пристроїв брандмауера (та будь-яких інших налаштованих технологій сповіщень).

● Крім того, можливість запитувати всі налаштовані пристрої брандмауера у відповідь на загрози SecureX, а потім використовувати їх у скоординованому захисті одним клацанням миші, що спрощує видимість і підвищує ефективність реагування.

3. Cisco Defense Orchestrator Cisco Defense Orchestrator — це хмарне рішення для керування, яке дозволяє керувати політиками безпеки та конфігураціями пристроїв у продуктах безпеки Cisco та хмарних продуктах безпеки.

Результат: Узгоджена політика та видимість завдяки оптимізації політик безпеки та керування пристроями у корпоративній мережі.

4. Cisco Secure Web Appliance (раніше Web Security Appliance) Secure Web Appliance використовує кілька технологій і надає користувачам SecureX бачення підключень із загрозами в Інтернеті. У SecureX інтеграція Secure Web Appliance з іншими джерелами глобальної інформації про загрози та внутрішньої видимості підтвердить і збагатить висновки Secure Web Appliance підтвердженою інформацією про загрози та локальними спостереженнями [13].

Результат: Захист корпоративної мережі від найпоширенішого вектора загроз, незалежно від того, чи переглядають користувачі веб-сторінки в офісі, у дорозі чи будь-де між ними [16].

5. Cisco Secure Workload (раніше Tetration) Cisco Secure Workload — це гібридне хмарне рішення для захисту робочого навантаження та мікросегментації, призначене для захисту обчислювальних екземплярів як у локальних центрах обробки даних, так і в публічних хмарах.

Результат: Краща видимість для захисту критичних робочих навантажень програми за допомогою підходу нульової довіри.

6. Cisco Secure Access від Duo Cisco Secure Access від Duo забезпечує багатофакторну автентифікацію, перевіряючи особу користувача та працездатність пристрою під час кожної спроби входу за допомогою моделі нульової довіри. У SecureX Secure Access від Duo забезпечує дії для оркестровки, щоб клієнти могли створювати автоматизовані робочі процеси.

Результат: Захист бізнесу, надавши довірений доступ до своїх програм і встановивши довіру пристрою [17].

13. Додаткові захищені ресурси Cisco. Доступ до кількох джерел аналізу загроз включено в безкоштовне ліцензування для SecureX. До них входить база даних TALOS, стандартна архітектура Cisco Secure Threat Intelligence Architecture та приватне сховище, куди користувачі можуть завантажувати власні дані про загрози, створені вдома чи отримані з інших джерел.

Необхідно також розглянути додаткові сторонні інтеграції з SecureX. У SecureX можна агрегувати та співвідносити інформацію про загрози, доступну від Cisco Talos, із мережевими даними та даними безпеки від Cisco та сторонніх продуктів безпеки, розгорнутих у організації. Він об’єднує дані про загрози та локальний контекст безпеки та керування в одному місці.

Підключивши існуючу інфраструктуру до Cisco Secure у SecureX, можна буде краще зрозуміти загрози та вплив на все середовище корпоративної мережі. SecureX забезпечує вбудовану або готову інтеграцію для сторонніх інструментів безпеки, а його відкриті API дозволяють третім сторонам створювати власні інтеграції, щоб зробити їх інструменти сумісними з SecureX. Кожне джерело глобальної чи локальної інформації забезпечується модулем, зв’язаним за допомогою ключа API.

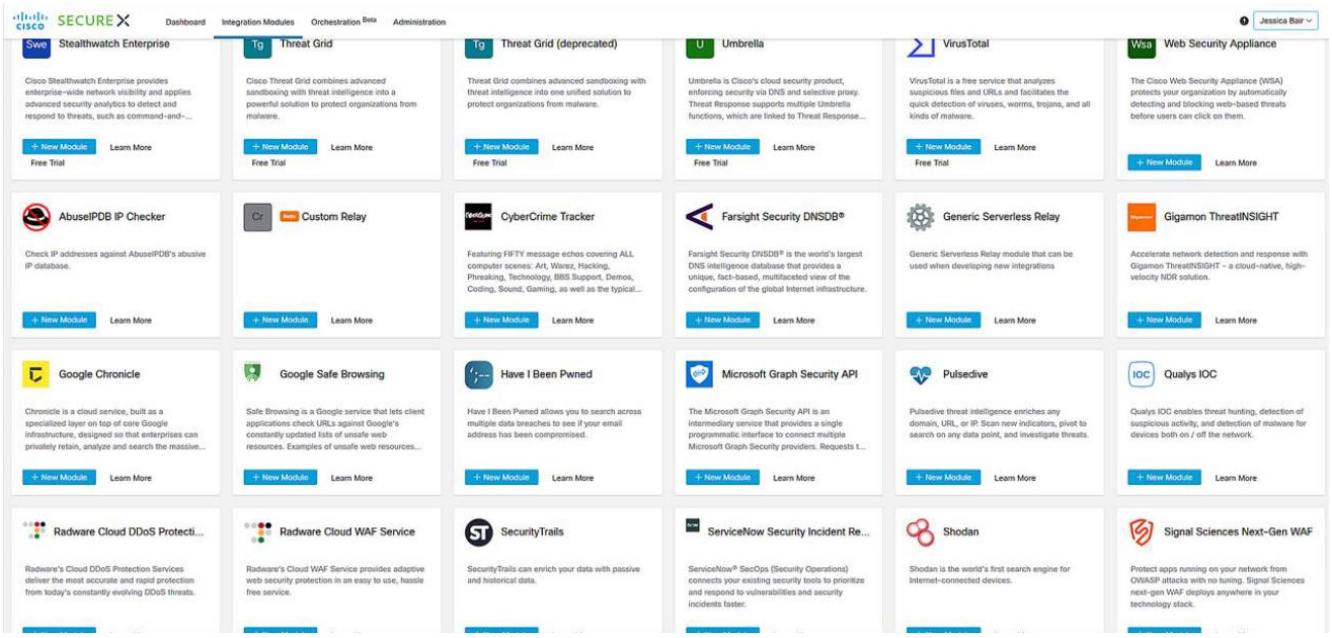

Рис. 2.5. Приклади програм для інтеграції із SecureX

Приклади використання для інтеграції наявних сторонніх інструментів із SecureX [13]:

- Агрегування та отримання інформації про загрози.
- Виявлення загроз.
- Реагування на інцидент.
- Автоматизація робочих процесів.

Таблиця 2.1

Основні сторонні партнери Cisco SecureX

Ключові сторонні партнери	Випадок використання
ServiceNow	● Джерело аналізу загроз – запит даних ServiceNow у відповідь на загрози SecureX ● Операційний – можливість надсилати запити/обмін даними реагування на загрози SecureX у ServiceNow Security Operations

Продовження таблиці 2.1

Основні сторонні партнери Cisco SecureX

IBM	● Операційний - запит/обмін даними відповіді на загрози SecureX у IBM QRadar Query IBM X-Force Exchange у відповідь на загрози SecureX.
Splunk	● Операційний – надсилання запитів та обмін даними реагування на загрози SecureX у Splunk Enterprise і Splunk Phantom
Microsoft	● Джерело аналізу загроз – надсилання запитів на дані Microsoft Graph Security у відповідь на загрози SecureX
Google	● Джерело аналізу загроз – запит даних Google Chronicle у відповідь на загрози SecureX

2.2. Аналіз функціональних можливостей та контролю безпеки корпоративної мережі на основі рішення Cisco SecureX

Функціональні можливості SecureX складаються з:

1. Стрічка SecureX — це транспортна основа для функціональності: вона дозволяє взяти з собою можливості SecureX та інтегрованих продуктів, коли настає необхідність переходу до будь-якої іншої консолі продукту. Це допомагає ділитися контекстом і підтримувати його, забезпечує єдиний досвід із широкими можливостями реагування.

Стрічкові програми – casebook, incidents і Orbital – створюються за посередництва SecureX і надаються SecureX та іншими продуктами.

Переваги [14]:

● Найрелевантніший контекст безпеки та розвідки про загрози для всіх продуктів.

● Власний інструменти під рукою, незалежно від того, на якій консолі перебуває система.

2. Відповідь на загрози SecureX — це основна програма для платформи, яка агрегує та співвідносить глобальну розвідку та локальний контекст у Cisco Secure і сторонні технології, в одному вигляді.

Переваги: Прискорення розслідування загроз і управління інцидентами для скорочення часу очікування загроз.

3. Оркестровка. Оркестровка SecureX із попередньо створеними робочими процесами, узгодженими зі звичайними випадками використання, і полотном коду, перетягуванням для створення власних робочих процесів, щоб усунути конфлікти у процесах корпоративної мережі і автоматизувати рутинні завдання.

Переваги:

● Прискорення часу для виправлення та автоматизації робочих процесів для зниження операційних витрат.

● Зменшення або усунення повторюваних завдань і розширення масштабів хмарної оркестровки.

● Зменшення людських помилок і покращення співпраці.

4. Статистика пристроїв. Статистика пристроїв SecureX забезпечує комплексну інвентаризацію кінцевих точок в єдиному уніфікованому поданні. Пошук кінцевих точок і звітування дозволяють оцінити конфігурацію безпеки пристрою на пристроях, що належать працівникам, підрядникам, компаніям, а також на пристроях IoT/OT — без ризику порушень роботи бізнес-процесів [14].

Переваги:

● Цілісне уявлення про дані пристроїв компанії, щоб спростити й автоматизувати дослідження безпеки.

● Можливість визначити прогалини в охопленні контролю, створювати власні політики та параметри автоматизації.

5. Інформаційна панель. Інформаційна панель SecureX – це перша сторінка, яку бачать користувачі після входу в систему. Вона дає єдиний огляд інфраструктури безпеки корпоративної мережі для уніфікованої видимості та зведених оперативних даних щодо безпеки середовища компанії.

Переваги:

● Можливість налаштування відповідно до того, що важливо корпоративній мережі, включаючи операційні показники.

● Відстеження нових загроз і доступ до нових продуктів одним натисканням.

6. Вхід. Вхід SecureX із багатофакторною автентифікацією Duo забезпечує доступ до всіх продуктів Cisco Secure за допомогою одного набору облікових даних з будь-якого пристрою, будь-де. Він забезпечує безпечну та стійку ідентифікацію, яка відповідає найвищим галузевим стандартам, включаючи FedRAMP, SOC 2 та ISO 27001.

Переваги:

● Легко отримати доступ до всіх програм компанії і підтримувати контекст за допомогою робочих процесів.

● Централізовано захищати та керувати обліковими даними на одному захищеному порталі.

7. Інтеграції. SecureX має вбудовану систему інтеграції з продуктами Cisco Secure, а також інтеграції з рішеннями сторонніх розробників за допомогою вбудованої, попередньо запакованої або спеціальної інтеграції для підключеної архітектури серверної частини та узгодженого зовнішнього інтерфейсу.

Переваги: Можливість спростити існуючу екосистему для підвищення ефективності загроз і меншого часу перебування загроз в системі компанії [18].

Рис. 2.6. Функціональні можливості SecureX

2.2.1. Ключова можливість: Стрічка

Частина філософії дизайну SecureX полягає в тому, що не потрібно переходити до кількох різних консолей, щоб отримати всі функції, необхідні для одного бізнес-завдання.

Стрічка SecureX втілює цю філософію в реальність у всьому портфоліо. Через стрічку, постійну панель у нижній частині інтерфейсу користувача всіх продуктів із підтримкою стрічки, наявний доступ до всіх функцій, наданих SecureX усіма розгорнутими технологіями компанії, сумісними з SecureX [15]. Стрічку можна згортати та розширювати, щоб відкривати програми стрічки, запускати інтегровані програми та переглядати профіль свого облікового запису. Зі стрічки є можливість переходити між SecureX або консоллю будь-якого інтегрованого продукту в будь-який інший інтегрований продукт. А також шукати на поточній веб-сторінці шкідливі хеші файлів, підозрілі домени та інші об’єкти кіберспостереження. Потім також можна додати спостереження випадку або дослідити знайдені в програмі реагування на загрози.

Стрічка дозволяє робити перехід, не виходячи, наприклад, з Secure Endpoint, щоб перейти до інтерфейсу Cisco Umbrella.

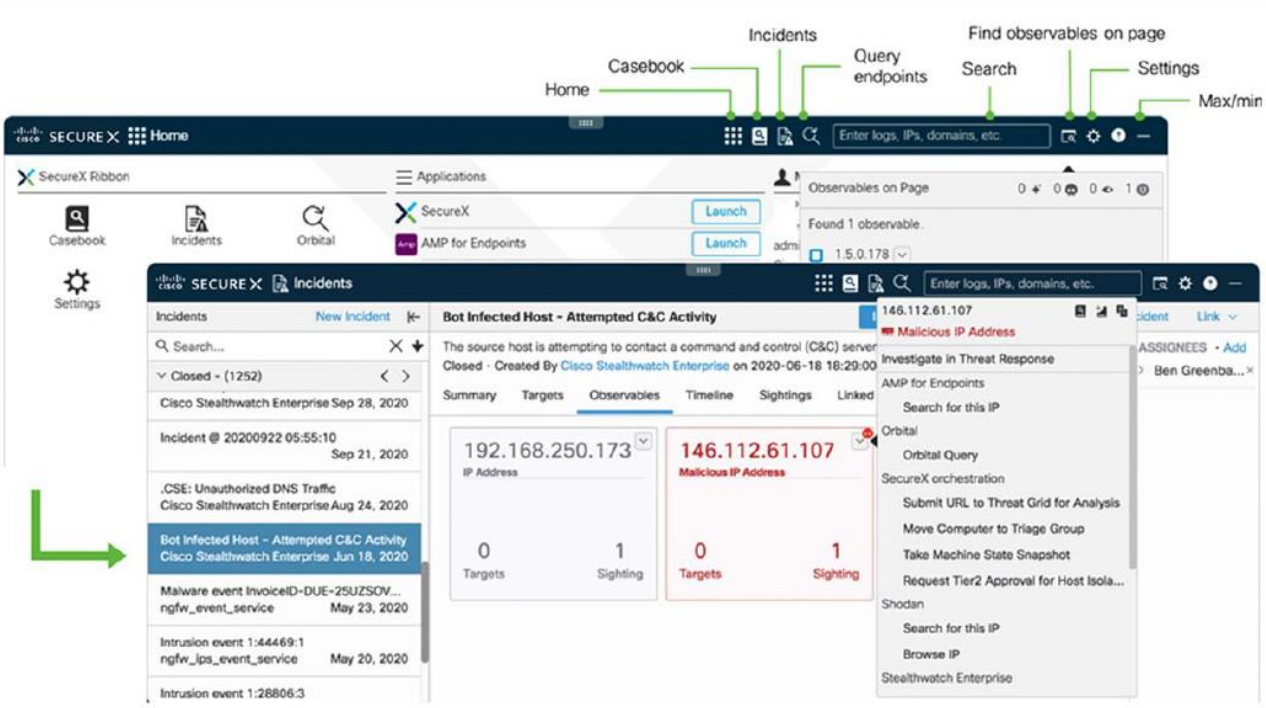

Рис. 2.7. Перехід між інтерфейсами інтеграцій

Стрічка — це уніфікований досвід, що надає доступ до можливостей усіх інтегрованих продуктів і дозволяє широкі дії реагування. Стрічка підтримує та надає доступ до контексту безпеки та аналізу загроз під час навігації між SecureX і всіма продуктами Cisco Secure. Стрічкові додатки розробляються за допомогою SecureX і можуть надаватися SecureX або іншими продуктами Cisco Secure. Список доступних програм:

- Інструмент Casebook, який дозволяє збирати спостережувані в групи, призначати випадку ім’я та опис, робити та зберігати нотатки про випадок, додавати інші спостережувані в будь-який час. Можливість негайно бачити результати, вживати заходів і ділитися справами між співробітниками. Усі справи в одній хмарній частині, яку легко знайти та поділитися.

- Інциденти. Автоматизування сортування та визначення пріоритетів сповіщень, які зараз надходять від Cisco Secure Firewall і Cisco Secure Network Analytics. Підтримувати єдиний список інцидентів безпеки для всіх підтримуваних продуктів; призначати, відкривати, закривати та працювати квитки протягом життєвого циклу; швидкий поворот до розслідувань і реагування, як

результат - економія часу і людських зусилль, досліджуючи події та збагачуючи їх контекстом із інтегрованих продуктів, визначаючи пріоритет реагування на надзвичайно термінові інциденти.

- Cisco Orbital Advanced Search, функції Secure Endpoint. Orbital забезпечує видимість кінцевих точок у звичному форматі SQL з інтуїтивно зрозумілим графічним інтерфейсом і каталогом попередньо створених запитів для виявлення загрози та реагування на інциденти, як результат – можливість за лічені секунди запускати глибокі та детальні запити про стан системи паралельно для всього розгортання.

2.2.2. Ключова можливість: Відповідь на загрози

Відповідь на загрози SecureX – це програма для розслідування безпеки та реагування на інциденти. Вона спрощує пошук загроз і реагування на інциденти, прискорюючи виявлення, розслідування та усунення загроз. Програма реагування на загрози надає контекст і вдосконалення ваших розслідувань безпеки шляхом підключення рішень безпеки Cisco (через кінцеву точку, мережу та хмару) та інтеграції з інструментами сторонніх розробників, все в одній консолі.

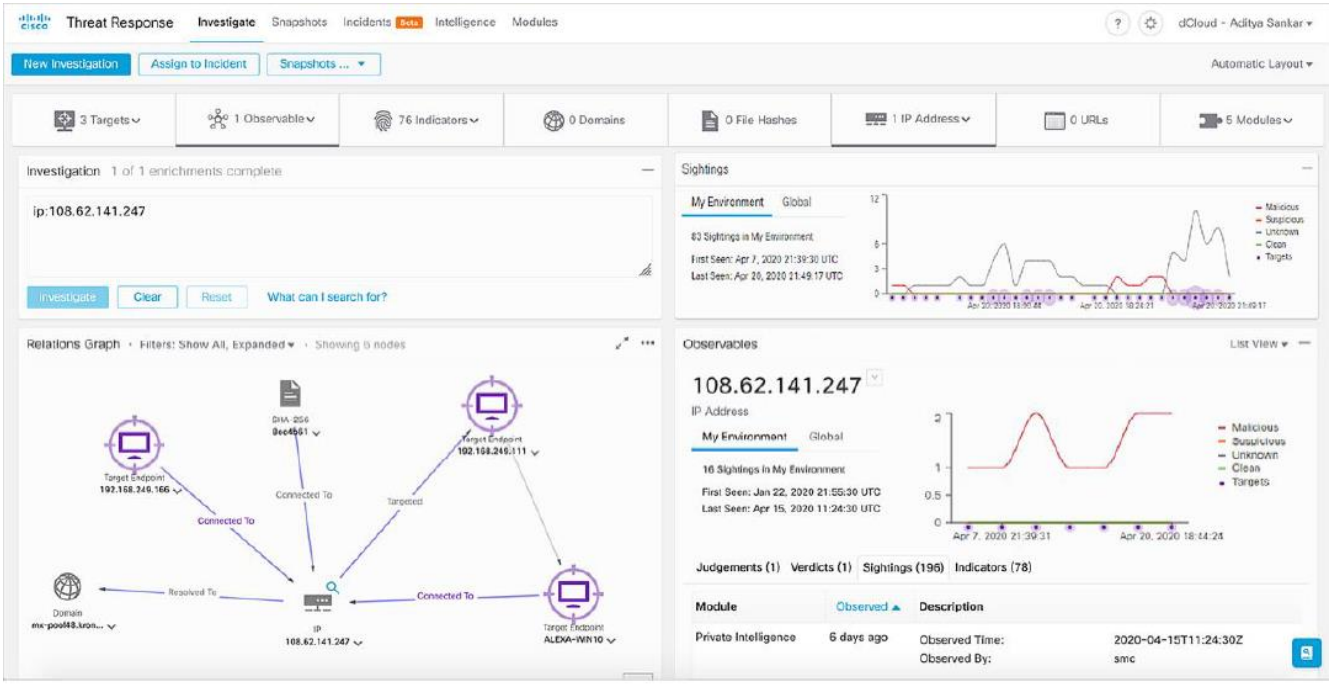

Рис. 2.8. Відповідь на загрози SecureX

Щоб зрозуміти, чи була загроза помічена у середовищі корпоративної мережі, а також її вплив, реакція на загрози SecureX об’єднує контекстну обізнаність із джерел даних продуктів безпеки Cisco разом із глобальною розвідкою про загрози від Talos і сторонніх джерел через API. Реакція на загрозу визначає, чи є такі спостережувані параметри, як хеші файлів, IP-адреси, домени та адреси електронної пошти, підозрілими чи зловмисними, і чи постраждали вони. Вона також надає можливість виправляти помилки безпосередньо з інтерфейсу та блокувати підозрілі файли, домени, ізолювати хости тощо без попереднього переходу до іншого продукту.

Таблиця 2.2

Основні функції можливості Відповіді на загрози

Функціонал	Опис	Перевага
Графік зв’язків	Візуалізація всіх спостережуваних загроз, знайдених під час дослідження, і вказує на зв’язки між ними	Легко визначати характер подій і стосунків.
Інциденти	Автоматизоване сортування та пріоритезація сповіщень від Cisco Secure Firewall і Cisco Secure Network Analytics	Дослідження подій та збагачення їх контекстом завдяки інтеграції продуктів безпеки, а також реагування на надзвичайно термінові інциденти
Плагін для браузера	Розширення для браузера, яке дозволяє отримувати IP-адреси або домени з будь-якого місця, де видно спостережувані інцеденти, для дослідження	Швидко та легко витягнути індикатори компрометації з будь-якої веб-сторінки чи консолі на основі браузера, Cisco чи іншої системи, і почати розслідування.

Продовження таблиці 2.2

Основні функції можливості Відповіді на загрози

Інструмент Casebook	Casebook для збереження, спільного використання та розширення аналізу загроз, який дозволяє документувати весь аналіз у хмарному середовищі та зберігати знімки з усіх інтегрованих або доступних через Інтернет інструментів.	Безпроблемне опрацювання інциденту за допомогою кількох інструментів, Cisco чи інших. Поліпшення співпраці між персоналом.
Знімки	Документування стану розслідування в певній організації на певний момент часу. Збереження поточного дослідження та графік для подальшого пошуку та аналізу	Покращення співпраці між персоналом. Збагачення розвідувальних даних, спостереження з місцевого контексту, спостережувані дані розвідки про загрози, зведені та зіставлені в одному поданні. Доступ до кількох джерел розвідки про загрози в одному поданні для прискорення розслідувань.
Дії реагування	Застосування захисних елементів керування, таких як: ● Блокування файлів ● Блокування URL-адрес ● Блокування доменів ● Ізоляція хостів ● Організовані робочі процеси	Відповідь на перший удар в одній консолі без переходу на інші консолі продукту

2.2.3. Ключова можливість: Статистика пристроїв

Завдяки функції Device Insights є можливість консолідувати інформацію з кількох диспетчерів пристроїв, інструментів виявлення та реагування на кінцеві точки та інших продуктів захисту кінцевих точок, а потім перенести надані ними деталі в уніфіковане подання в SecureX.

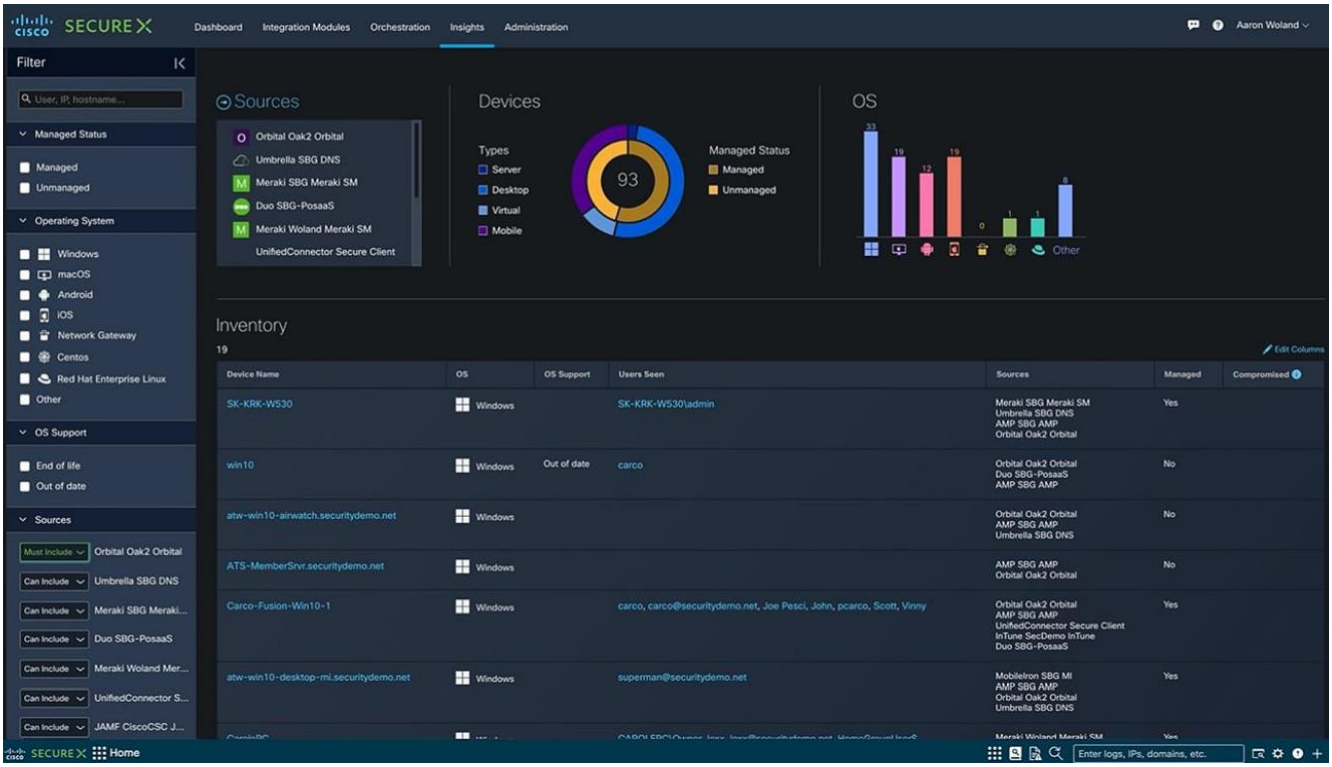

Рис. 2.9. Функція Device Insights

Device Insights допомагає виявити прогалини в охопленні контролем, розробити власні політики та дослідити можливості автоматизації на основі посібника. Існує можливість використовувати корельовані кінцеві точки для визначення контексту, щоб ідентифікувати та ізолювати кінцеві точки, які потрапили в пастку кібератак [11].

Device Insights також надає повну інвентаризацію кінцевих точок у SecureX. Можливо відстежувати інвентаризацію пристроїв і краще розуміти розширюваний і мінливий характер ландшафту кінцевих точок. Крім того, пошук кінцевих точок і звітування дозволяють оцінити конфігурацію безпеки пристроїв на пристроях,

що належать працівникам, підрядникам, а також на пристроях IoT/OT — без ризику порушення роботи бізнес процесів компанії.

Таблиця 2.3

Основні функції можливості Статистика пристроїв

Функціонал	Опис	Перевага
Джерела видимості активів	Візуалізація всіх джерел активів у корпоративній мережі, яка надає інформацію про продуктивність у часі та синхронізацію записів.	Цілісне уявлення про активи, підключені до корпоративної мережі.
Налаштування безпеки	Діаграми та таблиці конфігурації безпеки, які розбивають пристрої у мережевому середовищі та стан шифрування пристрою, брандмауера, блокування екрана, визначень AMP і портів SMB.	Легко відстежувати відповідність пристроїв у середовищі корпоративної мережі

Продовження таблиці 2.3

Основні функції можливості Статистика пристроїв

Інвентаризація	Повна інвентаризація пристроїв із детальною інформацією про ОС, користувачів, джерела, статус керування, модель пристрою та стан зламу. Можна отримати повну інформацію про один пристрій і переглянути повну історію його використання, хто ним користувався, а також отримати додаткову інформацію про вразливі місця пристрою та інциденти. Можна використовувати фільтри для створення спеціальних звітів, які можна експортувати у CSV.	Отримання детальної інформації про всі пристрої у корпоративній мережі. Можливість легко оцінити критичні вразливості та історію інцидентів

2.2.4. Основні можливості: Оркестровка

Оркестровка SecureX є ключовою можливістю в SecureX, автоматизовуючи повторювані та критичні завдання безпеки, такі як дослідження загроз, виявлення загроз та випадки їх використання. Оркестровка SecureX забезпечує заздалегідь створені робочі процеси та можливості реагування на інциденти, або надає

можливість створити власний за допомогою полотна коду та перетягування, щоб підвищити ефективність і точність роботи та знизити експлуатаційні витрати.

Оркестровка SecureX дає змогу визначати робочі процеси, які відображають типові процеси безпеки; етапи автоматизації (діяльності), логіку чи потік між цими кроками та спосіб передачі даних від одного кроку до наступного. За допомогою SecureX можливо використовувати Cisco Secure і багатодоменні системи, програми, бази даних і мережеві пристрої сторонніх виробників у корпоративному середовищі для створення цих робочих процесів.

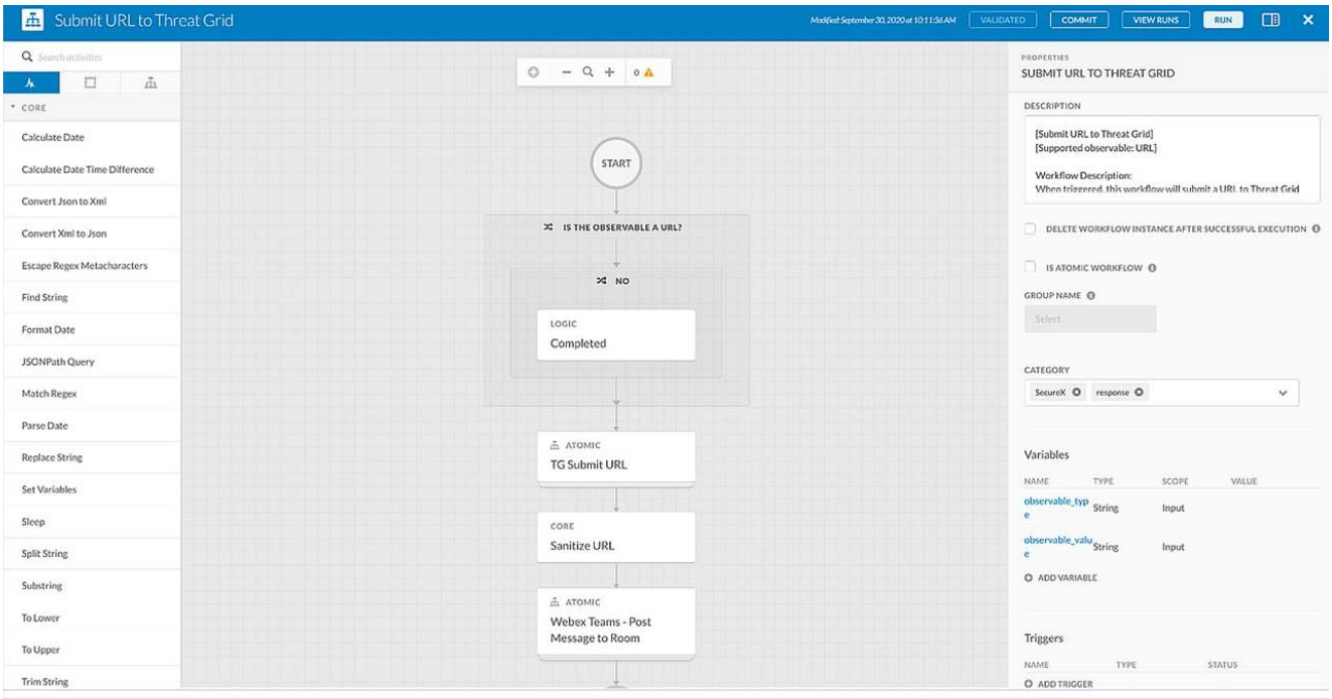

Рис. 2.10. Оркестровка SecureX

Таблиця 2.3

Приклади попередньо розроблених автоматизованих робочих процесів, які можна створити

Робочий процес	Для кого	Опис
Автоматизувати робочі процеси реагування на ініційовані події	SecOps	Автоматично витягувати нові параметри для спостереження з блогів про загрози, які SecOps читає, збагачувати та додавати параметри для спостереження у корпоративному середовищі, створювати новий випадок тільки якщо мета знайдена; прискорення реагування на загрози за допомогою ефективної інформації.
Автоматизувати робочі процеси для керування вразливістю	ITOps	Автоматично надсилайте запити кінцевим точкам для виявлення вразливостей і створюйте заявки на інциденти у вашому ITSM для посилення захисту від злому.

Продовження таблиці 2.3

Приклади попередньо розроблених автоматизованих робочих процесів, які можна створити

Оптимізування пропускної здатності VPN для захисту віддаленого доступу	NetOps	Автоматично відстежуйте навантаження головної частини VPN. Якщо надто високий, вимагайте авторизації від NetOps і автоматично розгортайте віртуальні головні вузли для масштабування за вимогою для збільшення трафіку віддалених працівників.

Оскільки оркестровка SecureX інтегрована в платформу Cisco Secure, вона також може покращити процеси розслідування та реагування за допомогою робочих процесів «відповіді». Ці робочі процеси можна запустити зі зведених меню в рамках реагування на загрози SecureX, стрічки SecureX і багатьох інших інтерфейсів продукту.

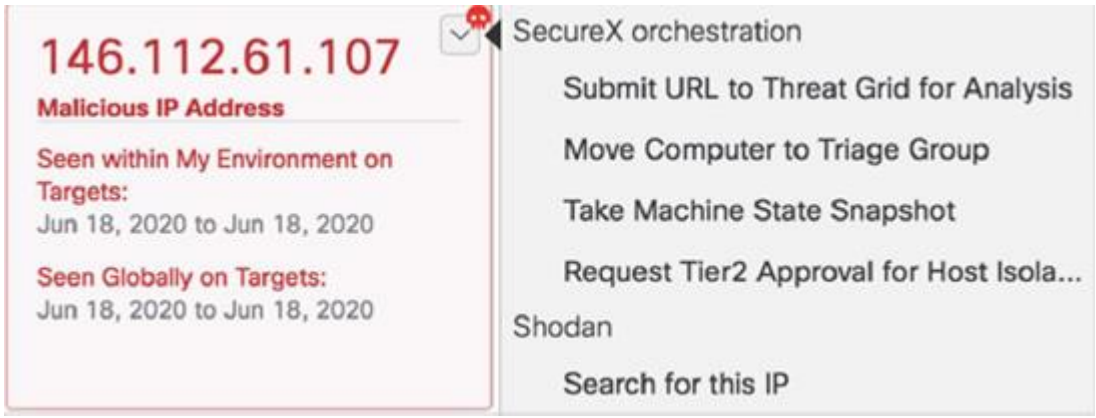

Рис. 2.11. Реагування за допомогою робочих процесів «відповіді»

Таблиця 2.4

Робочі процеси відповідей

Робочий процес	Опис
Переміщення комп'ютера до групи сортування	Необхідно взяти IP-адресу, ім'я хоста або GUID комп'ютера AMP і перемістити відповідну кінцеву точку до групи сортування.
Надіслати URL-адресу в таблицю загроз	Дозволити користувачеві надсилати URL-адресу в таблицю загроз
Зробити миттєвий знімок Orbital	Необхідно взяти IP-адресу, ім'я хоста або GUID комп'ютера AMP і запустити миттєвий знімок Orbital forensic для відповідної кінцевої точки.
Зробити криміналістичний знімок і ізолювати	Необхідно взяти IP-адресу, ім'я хоста або GUID комп'ютера AMP, зробити запит на орбітальний криміналістичний знімок для кінцевої точки, а потім увімкнути ізоляцію хоста AMP за допомогою дії відповіді
Ізоляція хоста кінцевої точки з рівнем 2	Необхідно взяти GUID комп'ютера AMP і подати запит на підтвердження, щоб увімкнути ізоляцію хоста для відповідної кінцевої точки, використовуючи дію відповіді для ізоляції хоста AMP реагування на загрозу SecureX.

2.2.5. Основні можливості: інформаційна панель

Інформаційна панель SecureX — це перше, що бачать користувачі після входу в SecureX. Він дає єдине уявлення про інфраструктуру безпеки корпоративної мережі для уніфікованої видимості та агрегованих ефективних даних у середовищі безпеки компанії.

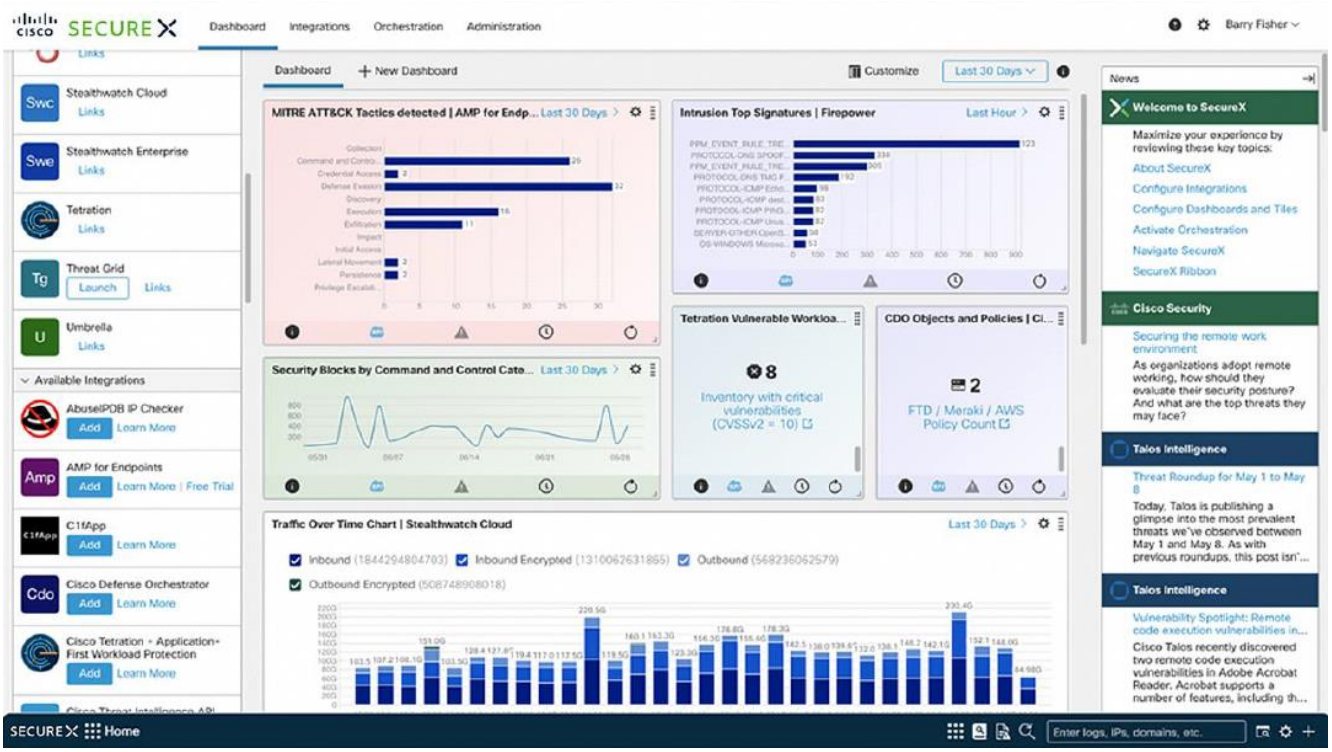

Рис. 2.12. Огляд інформаційної панелі

Огляд інформаційної панелі (рис. 2.12):

● На лівій верхній панелі: перегляд і запуск інтегрованих продуктів із посиланнями на ресурси підтримки

● На нижній лівій панелі: перегляд і самопідготовка тестів для інших доступних інтеграцій продуктів

● У центрі: налаштування до 20 настроюваних інформаційних панелей для кожного користувача, щоб переглядати показники та операційні заходи з інтегрованих продуктів у вашому середовищі безпеки

● На правій панелі: у стрічці новин користувачі можуть дізнатися про останні помітні загрози та інновації продукту

Висновки до другого розділу

Проаналізовано основні запити клієнтів та переваги використання рішення SecureX, яке об’єднує численні різнорідні датчики та технології виявлення порушень та вторгнень безпеки корпоративної мережі, а також забезпечує можливості оркестровки, що в свою чергу скорочує час виконання та обробки завдань повязаних з забезпеченням безпеки корпоративної мережі.

Вивчено та наведені можливі інтеграції SecureX з продуктами Cisco та продуктами сторонніх вендорів.

Досліджено функціональні можливості контролю безпеки корпоративної мережі на основі рішення Cisco SecureX такі як, стрічка, оркестровка, відповідь на загрози, інформаційна панель та наведені їх переваги.

3 ІНТЕГРАЦІЇ ТА НАЛАШТУВАННЯ РОБОТИ НА ОСНОВІ РІШЕННЯ CISCO SECUREX

3.1. Інтеграція Cisco Secure Firewall Management Center та SecureX

Налаштування центру керування, дозволяє керованим пристроям захисту від загроз надсилати підтримувані події безпосередньо до Exchange Services Exchange (SSE) у хмарі Cisco. Використовуючи SSE, можливо автоматично або вручну висвітлювати події як інциденти в SecureX.

Можливо також переглянути стан системи, наприклад, чи встановлено на пристроях поточні версії програмного забезпечення.

Пряма інтеграція підтримує такі типи подій [19]:

- Події вторгнення
- Події підключення служби безпеки
- Файли та шкідливі події

На рисунку 3.1 показано, як працює пряма інтеграція.

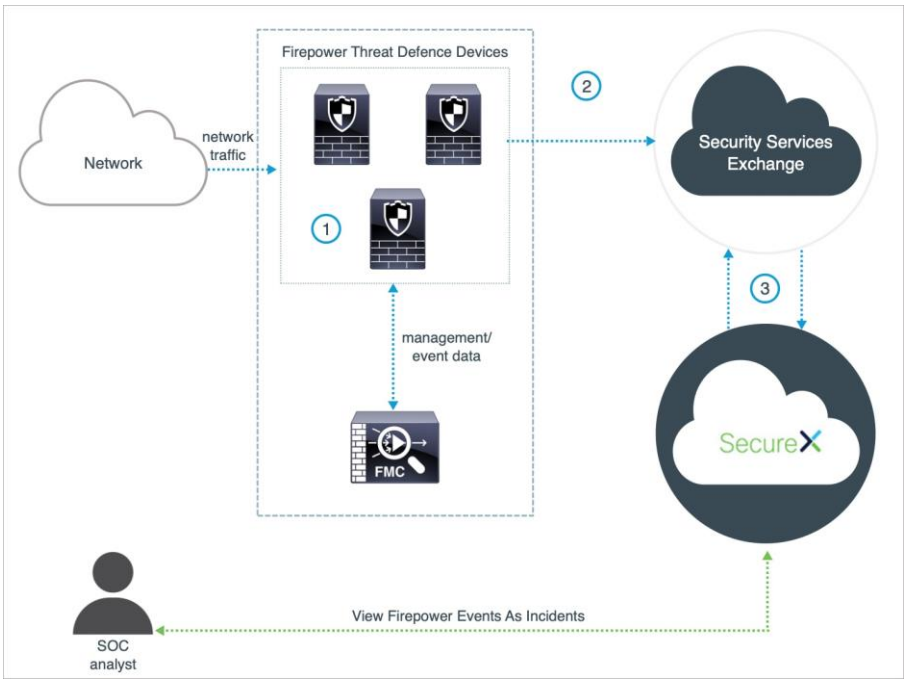

Рис. 3.1. Принцип роботи прямої інтеграції

1. Пристрої, якими керує центр керування, генерують події.

2. Пристрої захисту від загроз надсилають події до SSE.

3. SecureX запитує SSE про спостереження, пов’язані з IP-адресою, що досліджується, і надає аналітику SOC додатковий контекст. Події автоматично або вручну підвищуються до інцидентів, які відображаються в SecureX.

Ключові компоненти цієї інтеграції:

1. SecureX – спрощена платформа, яка поєднує інтегрований портфель безпеки Cisco з наявною інфраструктурою. Це допомагає уніфікувати видимість, увімкнути автоматизацію та посилити безпеку в мережі, кінцевих точках, хмарі та програмах

2. Security Services Exchange (SSE) - Захищений проміжний хмарний сервіс, який обслуговує ідентифікацію, автентифікацію та зберігання даних із хмари в хмару та з приміщення в хмару для використання в продуктах безпеки Cisco у хмарі

3. Вхід SecureX - Захищена сторінка входу для доступу до всіх ваших продуктів Cisco Security за допомогою одного набору облікових даних із будь-якого пристрою

4. Мережа успіху Cisco (CSN) - хмарна служба, активована користувачем, яка встановлює безпечне з’єднання з хмарою Security Service Exchange (SSE) для потокової передачі інформації про використання Firepower і статистики

5. Відповідь на загрозу Cisco SecureX - хмарна платформа, яка допомагає виявляти, досліджувати, аналізувати загрози та реагувати на них, використовуючи дані, зібрані з багатьох продуктів і джерел.

Щоб інтегрувати центр керування та керовані пристрої захисту від загроз із SecureX необхідно виконати послідовності наведені на рис.3.2.

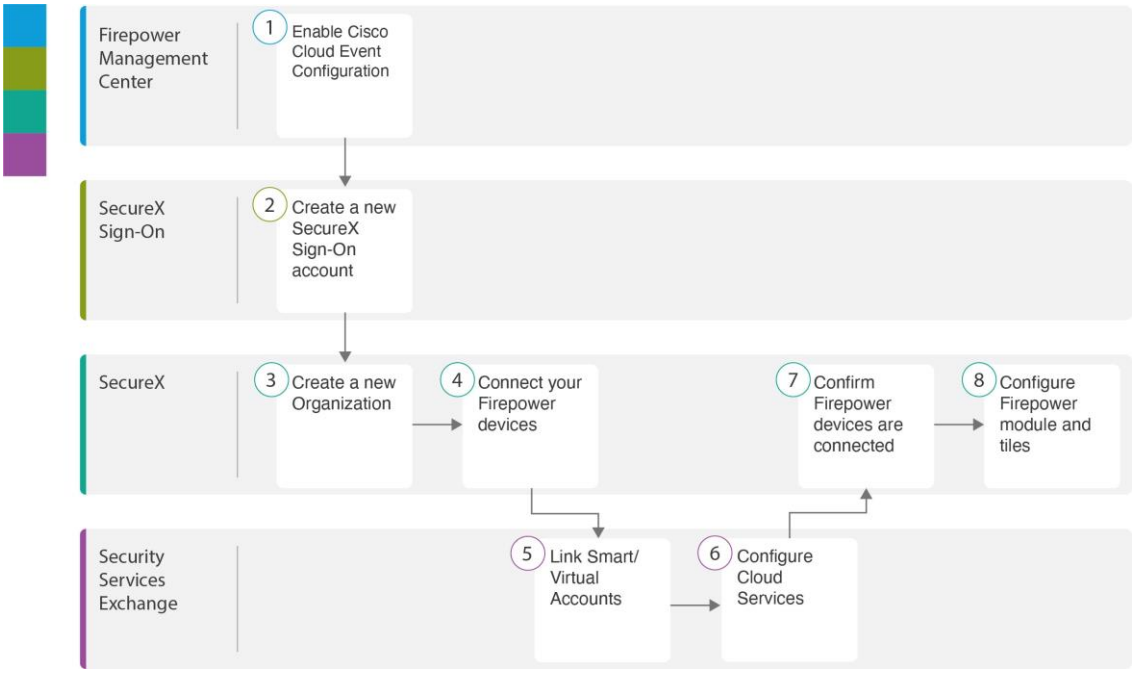

Рис. 3.2. Послідовність дій для успішної інтеграції

3.1.1. Налаштування Secure Firewall Management Center для надсилання подій до Security Services Exchange

Налаштувати свій центр керування необхідно таким чином, щоб керовані пристрої захисту від загроз надсилали події безпосередньо до SSE .

У центрі керування необхідно виконайти такі дії [19]:

- Натиснути «Система» → «Конфігурація» та призначити своєму центру керування унікальне ім’я, щоб було чітко ідентифіковано у списку пристроїв у хмарі.
- Додати пристрої захисту від загроз до центра керування, призначити їм ліцензії та переконатися, що система працює належним чином. (Тобто створили необхідні політики, а події генеруються та відображаються належним чином у веб-інтерфейсі центру керування на вкладці «Аналіз».)

Процедура:

1. У веб-інтерфейсі центру керування натиснути «Система» → «Інтеграція».
2. У віджеті Cisco Cloud Region у випадаючому списку «Регіон» вибирати регіональну хмару та натиснути «Зберегти» .

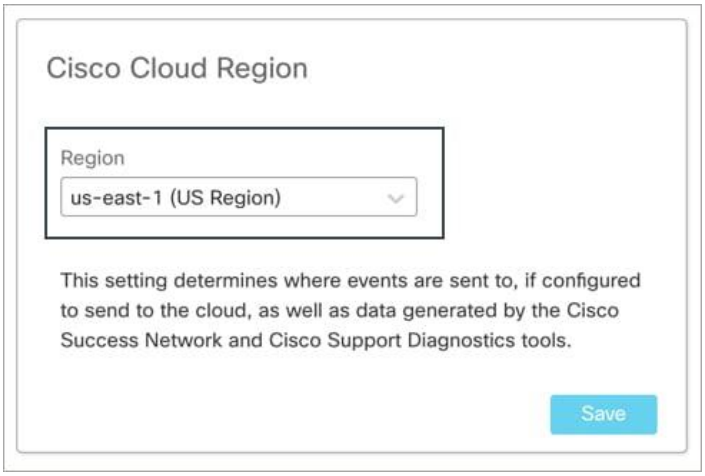

Рис. 3.3. Віджет Cisco Cloud Region

Перш ніж вибрати регіональну хмару, необхідно звернути увагу на такі важливі моменти:

- Дані в різних хмарах не можна агрегувати або об’єднувати.
- Якщо потрібно агрегувати дані з кількох регіонів, пристрої в усіх регіонах мають надсилати дані до однієї регіональної хмари.

Можна створити обліковий запис у кожній регіональній хмарі. Дані про кожну хмару будуть окремо.

Якщо центр керування вже зареєстровано у вибраній регіональній хмарі, кнопка «Зберегти» буде неактивною.

3. У віджеті Cisco Cloud Event Configuration налаштувати центр керування для надсилання подій до SSE.

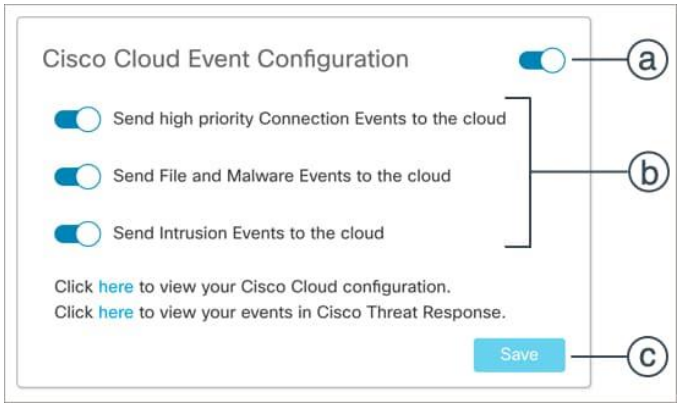

Рис. 3.4. Віджет Cisco Cloud Event Configuration

a. Натиснути повзунок Cisco Cloud Event Configuration, щоб увімкнути конфігурацію.

b. Увімкнути або вимкнути типи подій для надсилання до SSE.

c. Натиснути Зберегти.

3.1.2. Налаштування нового облікового запису SecureX для входу

За допомогою облікового запису SecureX Sign-On можливо легко отримати доступ до всіх корпоративних продуктів Cisco Security за допомогою одного набору облікових даних із будь-якого пристрою.

Процедура:

1. Вхід SecureX: необхідно зареєструвати новий обліковий запис SecureX Sign-On

- Перейти на сторінку https://sign-on.security.cisco.com.
- Натиснути «Створити вхід SecureX».

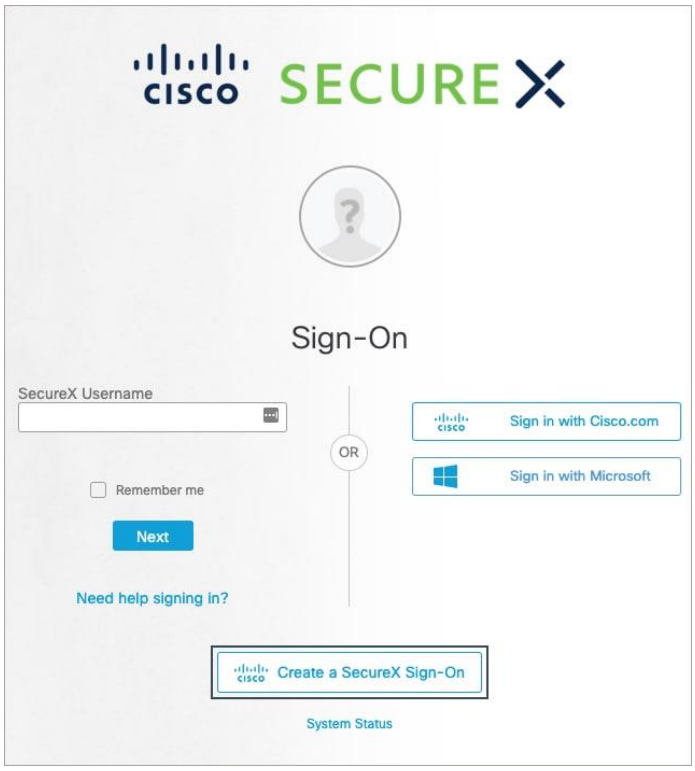

Рис. 3.5. Форма створення облікового запису

- Необхідно заповнити форму та натиснути Зареєструватися.

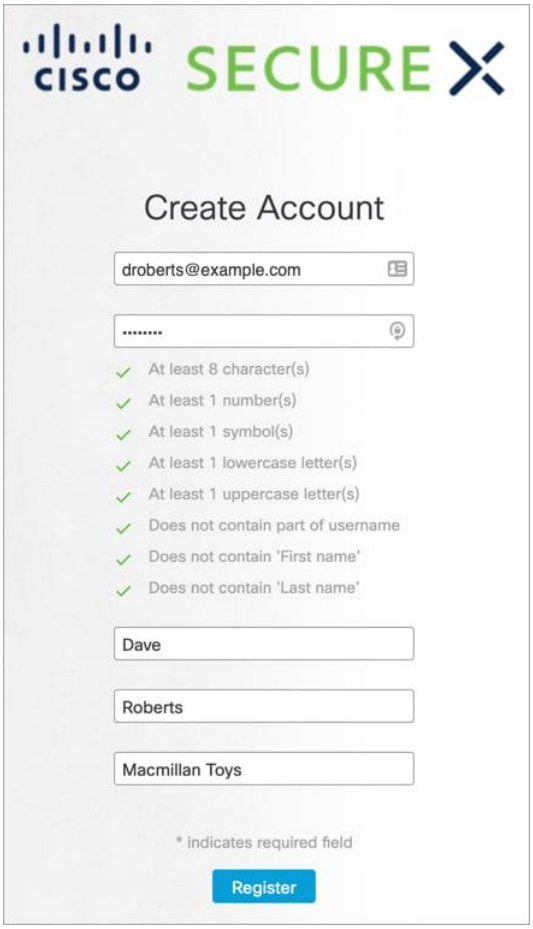

Рис. 3.6. Заповнення форми реєстрації

- Необхідно знайти електронний лист для активації облікового запису та натиснути «Активувати обліковий запис».

2. Вхід SecureX: налаштувати багатофакторну автентифікацію (MFA), налаштувавши Duo Security:

- На екрані «Налаштувати багатофакторну автентифікацію» натиснути «Налаштувати»

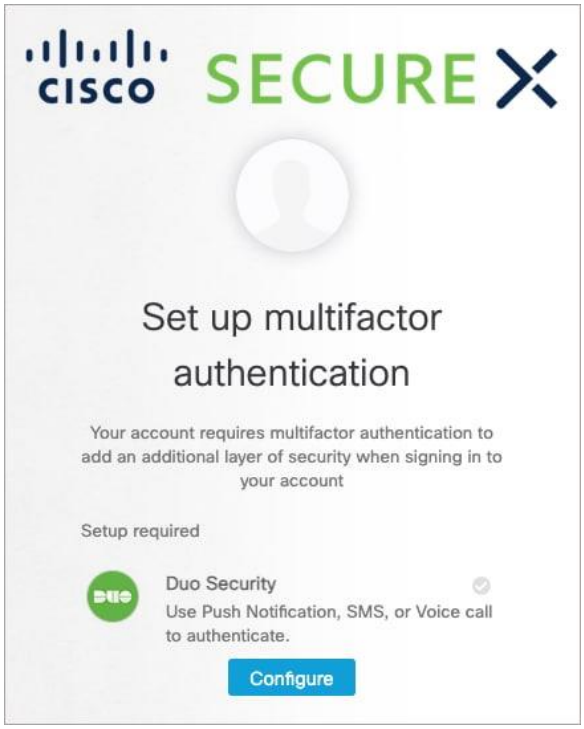

Рис. 3.7. Налаштування багатофакторної автентифікації

- Необхідно натиснути «Почати налаштування» та дотримуватися підказок, щоб вибрати пристрій і перевірити з'єднання цього пристрою з обліковим записом. Якщо уже є програма Duo на пристрої, отримаєте код активації для цього облікового запису. Duo підтримує кілька облікових записів на одному пристрої.
- Наприкінці майстра натиснути «Продовжити до входу».
- Увійти у SecureX Sign-On за допомогою двофакторної автентифікації.
- Після того, як пристрій підключено до облікового запису, натиснути «Готово». Крім того, наявні користувачі Google Authenticator для MFA можуть додати його сюди як резервний фактор, натиснувши Налаштувати Google Authenticator і дотримуючись підказок.

3. Вхід SecureX : налаштувати параметри відновлення облікового запису для свого облікового запису SecureX Sign-On.

- (Необов'язково) Додати номер телефону для зміни пароля або розблокування облікового запису за допомогою SMS.
- Обрати образ безпеки.

- Натиснути Створити обліковий запис. Якщо поточний сеанс минув до того, як налаштуються параметри відновлення облікового запису, SecureX Sign-On запропонує налаштувати їх під час наступного входу

4. SecureX: Створити нову організацію в SecureX.

- Обрати свій регіон для запуску SecureX.

- Якщо буде запропоновано, необхідно пройти автентифікацію за допомогою облікового запису SecureX Sign-On.

- Заповнити форму та натиснути Створити організацію.

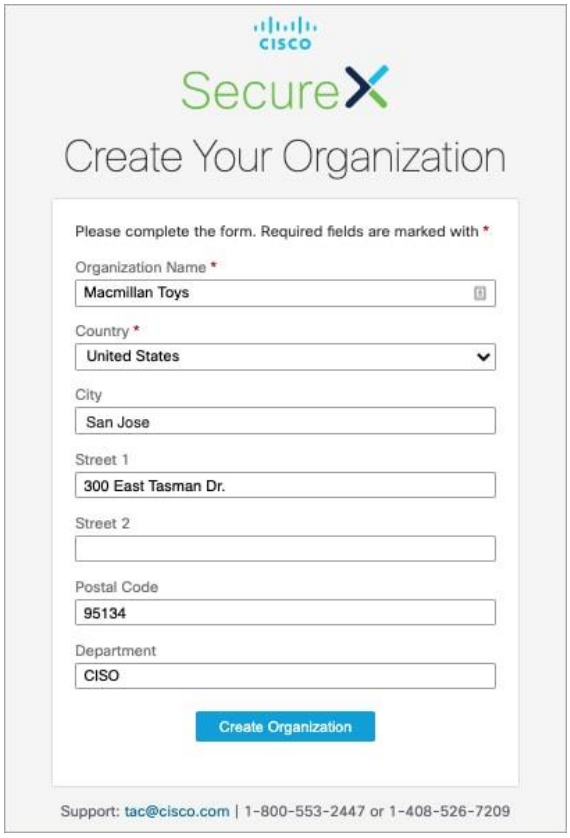

Рис. 3.8. Створення облікового запису

5. SecureX : перевірити дані нового облікового запису на SecureX

- Натиснути своє ім’я у верхньому правому куті сторінки активації облікового запису.

- Натиснути назву організації

- Перевірити дані свого облікового запису

3.1.3. Активація облікового запису SecureX Sign-On

Щоб почати використовувати SecureX, необхідно активувати обліковий запис SecureX Sign-On, підключивши принаймні один із пристроїв Firepower до SecureX.

Щоб зв’язати облікові записи ліцензування, необхідно мати права адміністратора на рівні Smart Account або Virtual Account для всіх облікових записів ліцензування (з яких ліцензуються ваші продукти Firepower) і для облікового запису, який використовується для доступу до SecureX.

Процедура:

1. Вхід у SecureX: доступ до SecureX:

- Перейти на сторінку https://sign-on.security.cisco.com/
- Увійти, використовуючи свій обліковий запис SecureX Sign-On
- Якщо буде запропоновано, пройти автентифікацію за допомогою Duo Security
- Обрати необхідний регіон для запуску SecureX

2. SecureX: ініціювати процес активації облікового запису SecureX.

- На сторінці активації облікового запису натиснути «Підключити»

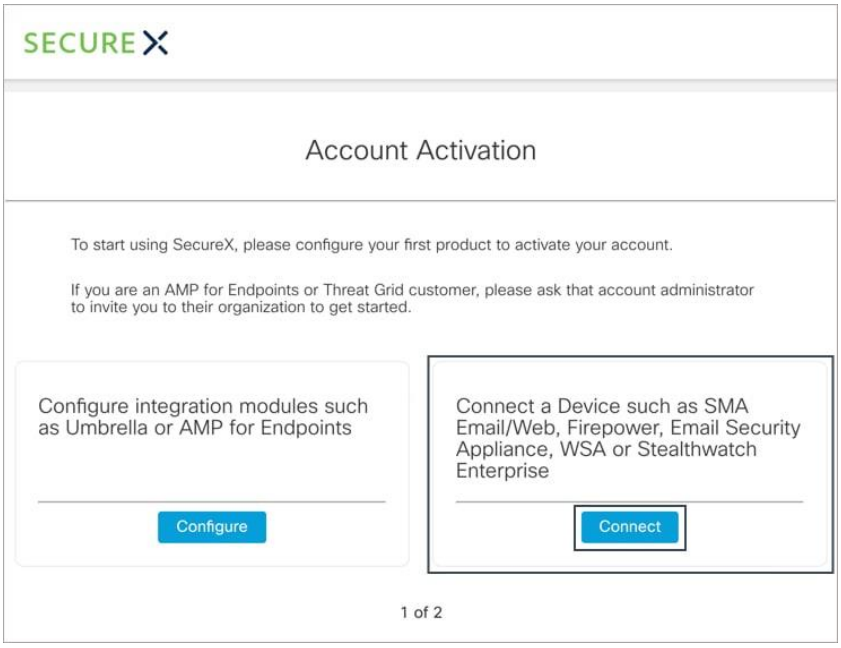

Рис. 3.9. Форма активації

- На сторінці «Підключити пристрій» натиснути «Під’єднати обліковий запис»

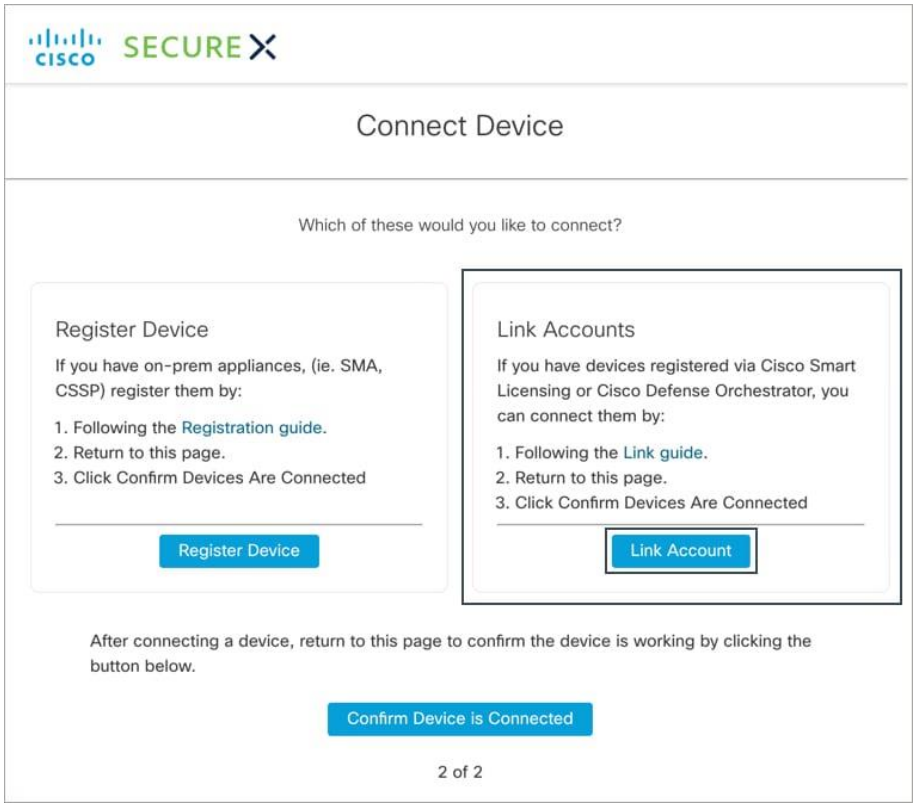

Рис. 3.10. Форма підключення пристроїв

3. Обмін службами безпеки : щоб інтегрувати продукти, зареєстровані за різними ліцензійними обліковими записами Smart (або віртуальними обліковими записами), в єдине представлення в хмарі, необхідно пов’язати ці облікові записи ліцензування з обліковим записом, який використовує компанія для доступу до SecureX.

- Увійти у SSE за допомогою облікового запису SecureX Sign-On [20]
- У верхньому правому куті натиснути кнопку «Інструменти» і обрати «Пов’язати розумні/віртуальні облікові записи»

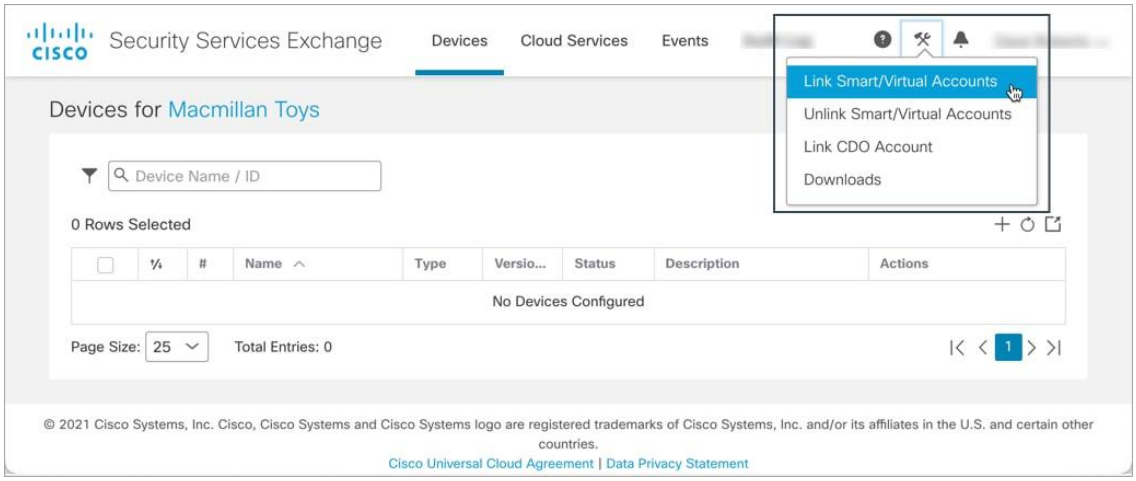

Рис. 3.11. Форма підключення акаунтів

- Натиснути Пов’язати інші облікові записи
- Якщо буде запропоновано, увійти, використовуючи облікові дані Cisco.com
- Обрати облікові записи для інтеграції з цим хмарним обліковим записом

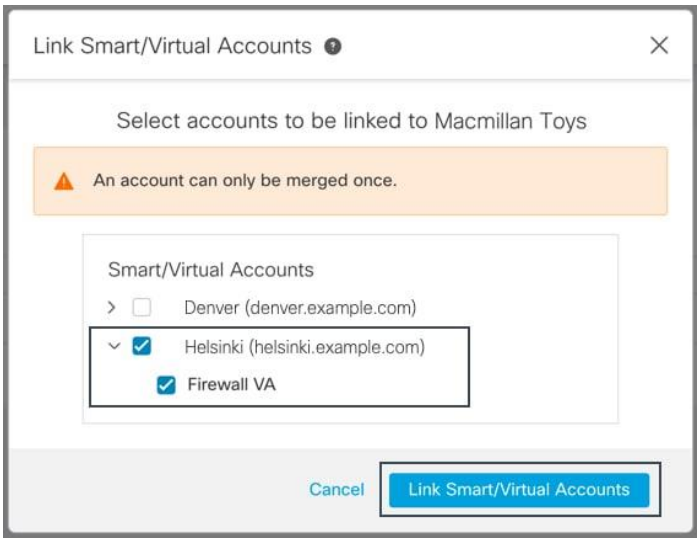

Рис. 3.12. Форма підключення облікових записів для інтеграції

- Натиснути Пов’язати розумні/віртуальні облікові записи
- Натиснути ОК , щоб продовжити
- Переконатися, що центр керування та керовані ним пристрої відображаються на вкладці «Пристрої»

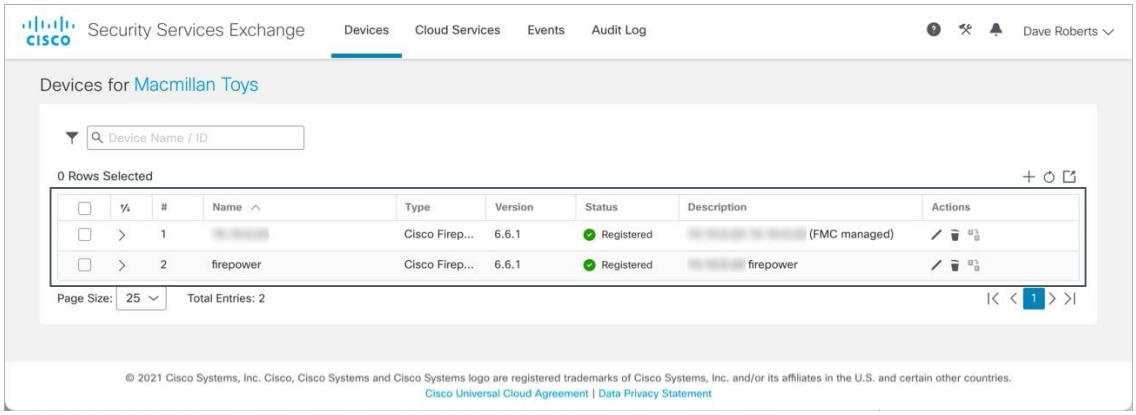

Рис. 3.13. Форма керування пристроями

- Переконатися, що події відображаються на вкладці Події

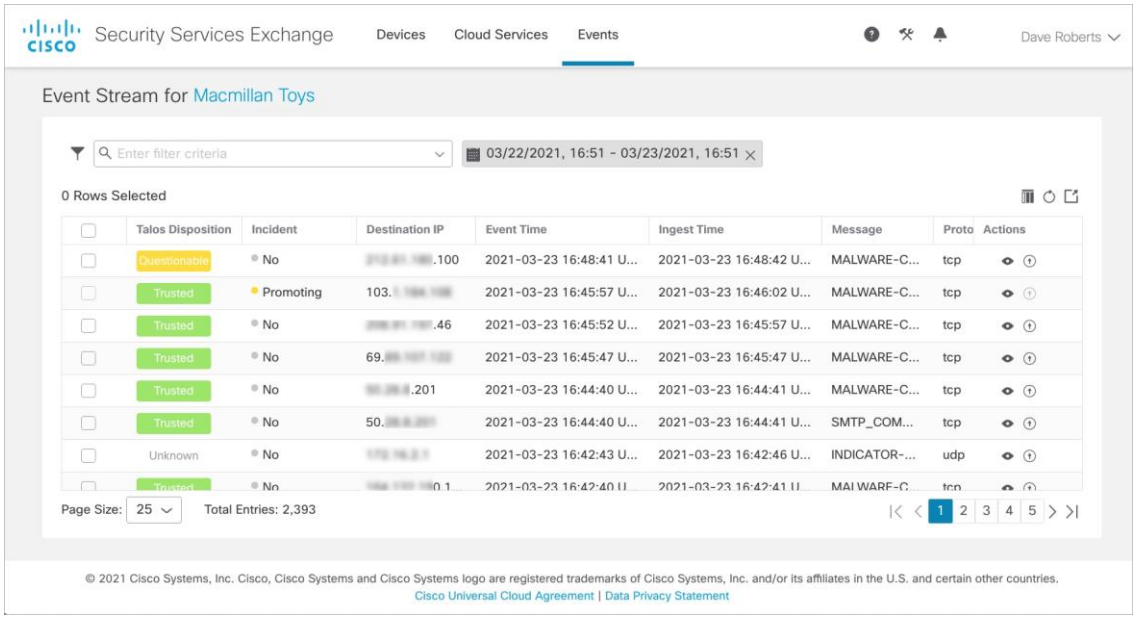

Рис. 3.14. Форма відображення подій

4. Security Services Exchange : налаштувати параметри хмарних служб у SSE

- Перейти на вкладку Хмарні служби
- Переконатися, що служби реагування на загрози Cisco SecureX і служби подій увімкнено

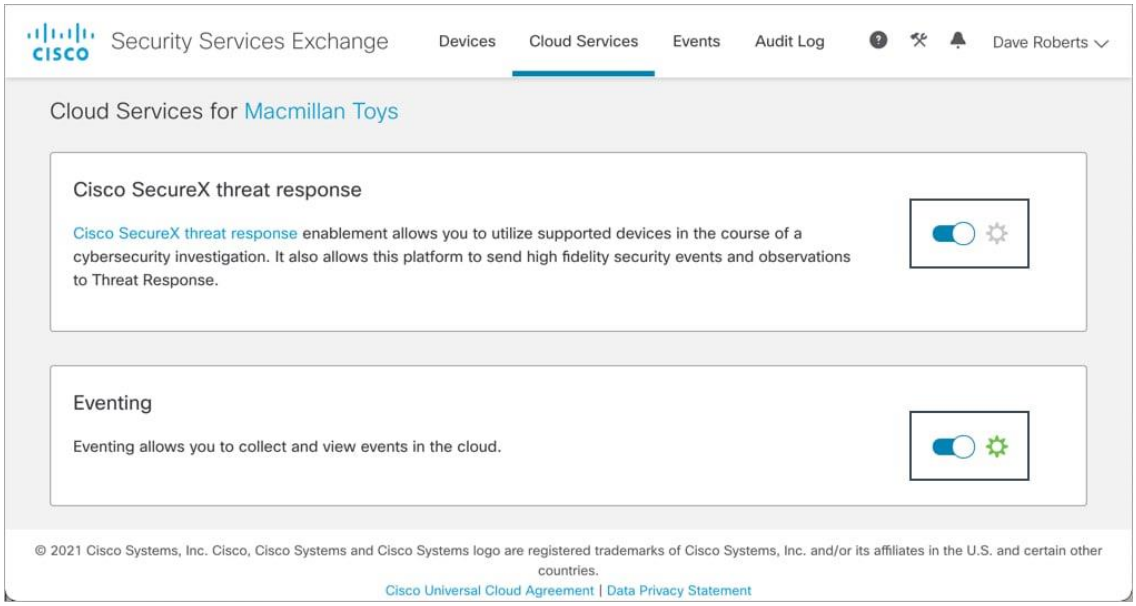

Рис. 3.15. Віджет Хмарні служби

- Щоб відслідковувати зловмисне програмне забезпечення та події Security Intelligence як інциденти в SecureX, натиснути під панеллю «Події», вибрати потрібні типи подій на вкладці «Автоматичне просування подій» і натиснути «Зберегти»

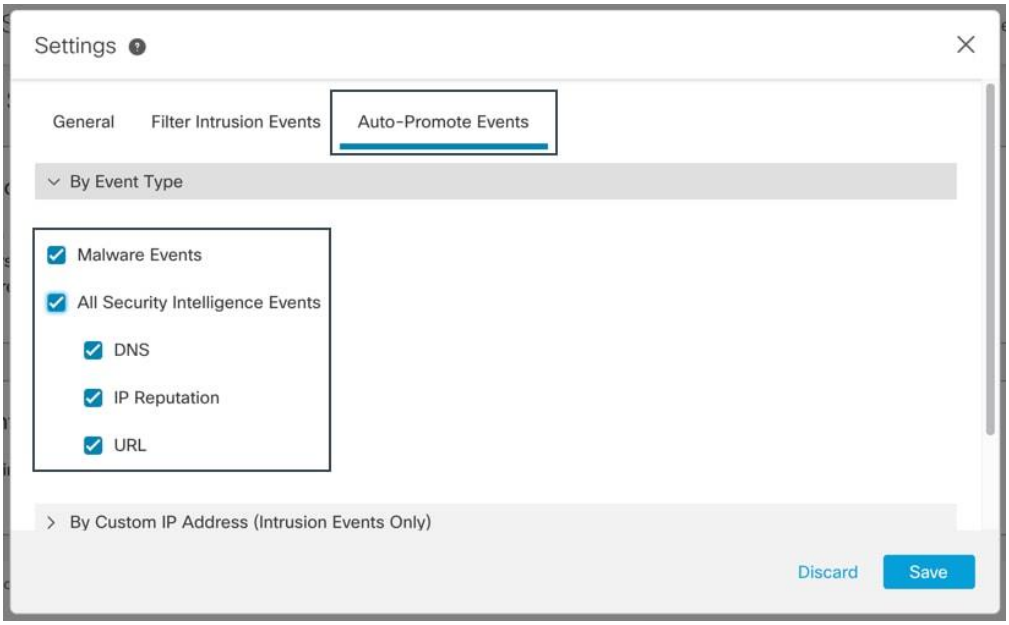

Рис. 3.16. Вкладка Автоматичне просування подій

5. SecureX: завершення процесу активації облікового запису SecureX.

- Повернутися на вкладку SecureX (сторінка «Підключити пристрій») і натиснути «Підтвердити підключення пристрою».
- Натиснути Почати використання SecureX.
- Перейти до «Адміністрування» -> «Пристрої» та переконатися, що центр керування та керовані ним пристрої відображаються на цій сторінці.

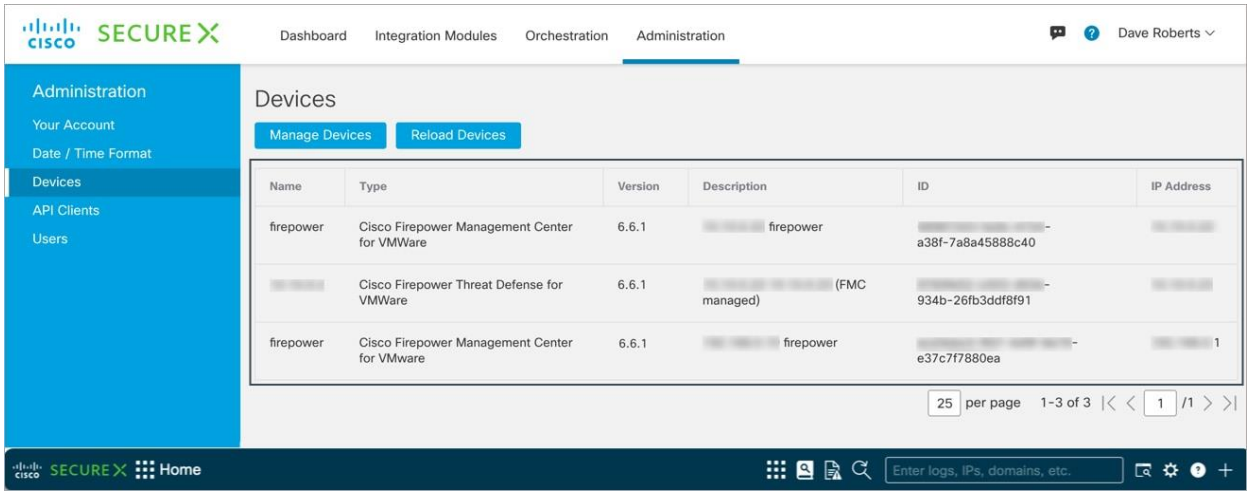

Рис. 3.17. Вкладка Адміністрування

3.1.4. Налаштування модуля Firepower і плитки в SecureX

Плитки SecureX представляють показники та дані з ваших продуктів Firepower, щоб забезпечити видимість у корпоративному середовищі безпеки та прискорити реагування на загрози. Після додавання модуля інтеграції Firepower у SecureX можна додати плитки Firepower на інформаційну панель.

Щоб переглянути плитки SecureX , які показують інформацію про систему, наприклад, чи працюють корпоративні пристрої з оптимальними версіями, увімкніть Cisco Success Network (CSN) у центрі керування.

Щоб перевірити або ввімкнути цей параметр, натиснути «Система»>«Розумні ліцензії» у веб-інтерфейсі центру керування.

Процедура [19]:

1. Вхід у SecureX: доступ до SecureX

- Перейти на сторінку https://sign-on.security.cisco.com/

- Увійти, використовуючи корпоративний обліковий запис SecureX Sign-On
- Якщо буде запропоновано, пройти автентифікацію за допомогою Duo Security
- Вибрати свій регіон для запуску SecureX

2. SecureX: додавання нового модулю інтеграції Firepower

- Перейти на вкладку «Модулі інтеграції»
- Натиснути «Додати новий модуль інтеграції»

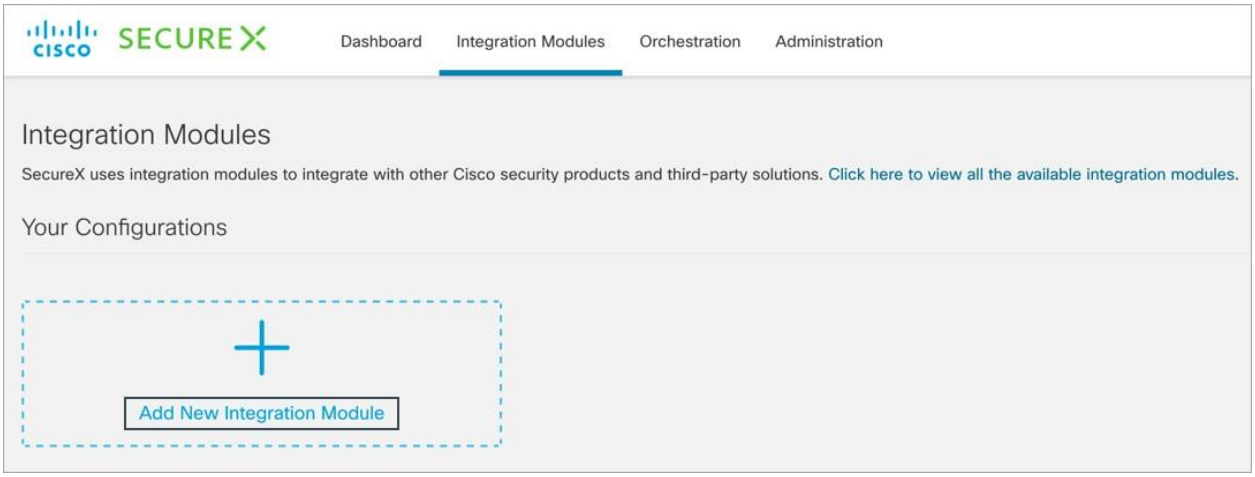

Рис. 3.18. Вкладка Модуль інтеграції

- Перейти до модуля інтеграції Firepower і натиснути + Новий модуль

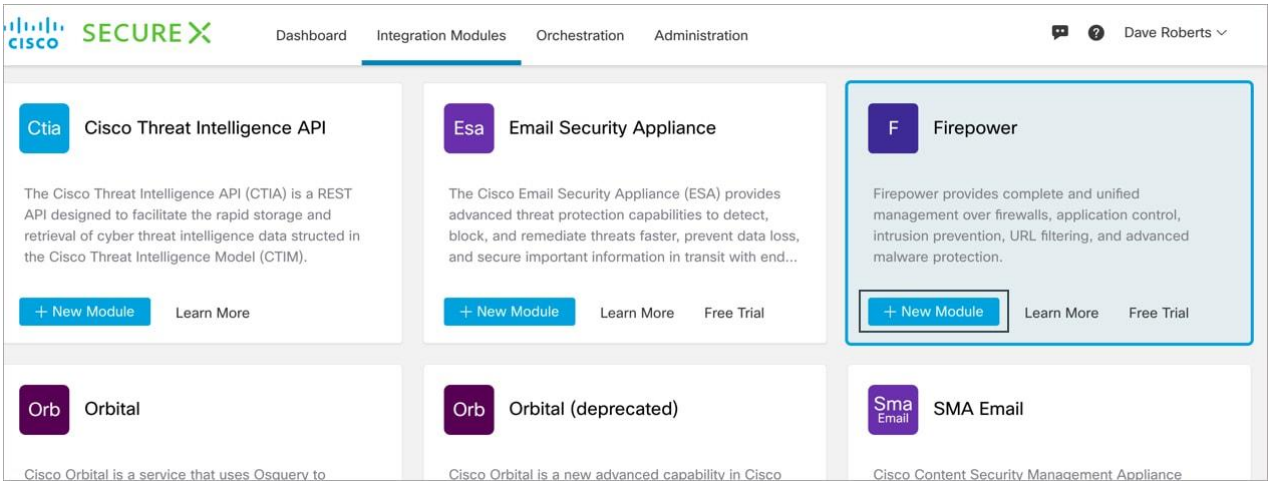

Рис. 3.19. Віджет Новий модуль інтеграції

- Ввести назву для модуля інтеграції Firepower і натиснути «Зберегти»

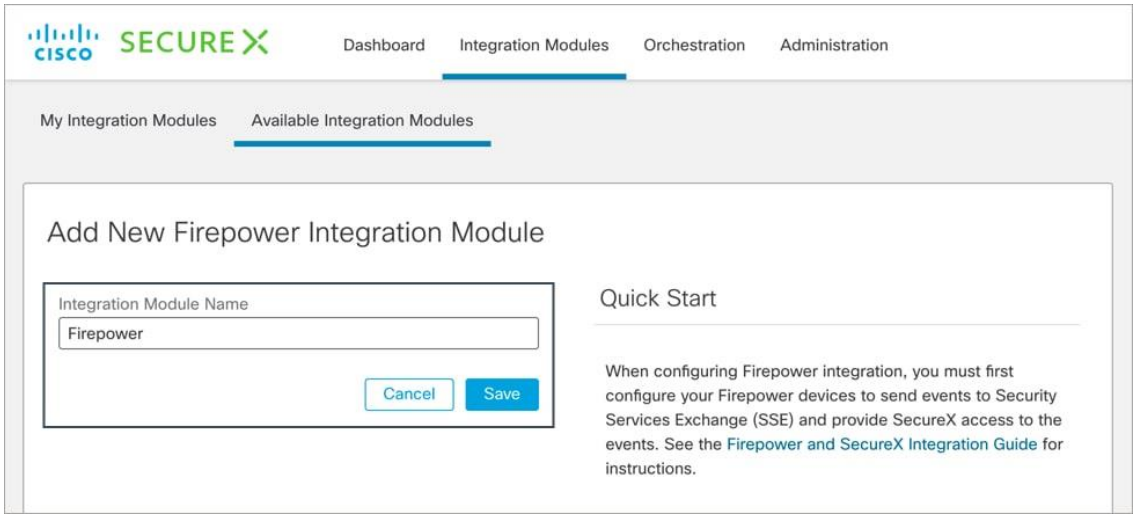

Рис. 3.20. Створення нового модулю інтеграції

Перевірка працездатності виконується, щоб визначити, чи модуль було налаштовано успішно. Після завершення цього процесу з’явиться повідомлення про відсутність проблем із конфігурацією або виявлення помилок.

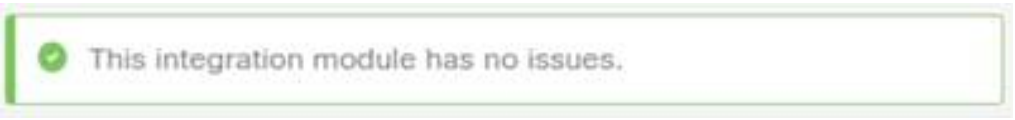

Рис. 3.21. Успішна перевірка працездатності

Після перевірки доданий модуль відображається на сторінці «Мої модулі інтеграції» (на вкладці «Модулі інтеграції»).

3. SecureX: додавання плитки FirePower

- Перейти на вкладку Інформаційна панель
- Натиснути «Додати плитки»
- Щоб створити нову інформаційну панель, натиснути «Створити інформаційну панель»

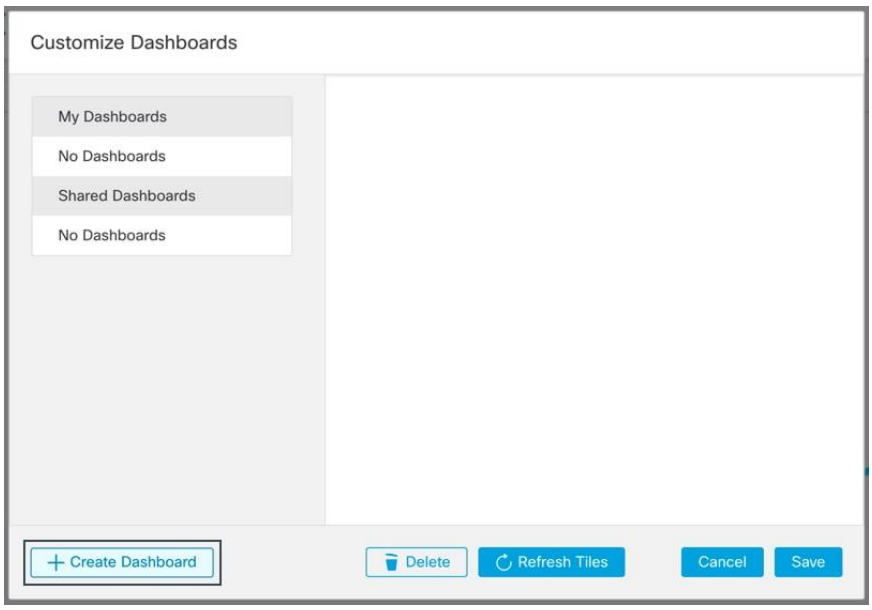

Рис. 3.22. Створення інформаційної панелі

- Ввести ім’я для інформаційної панелі, вибрати потрібні елементи Firepower і натиснути «Зберегти»

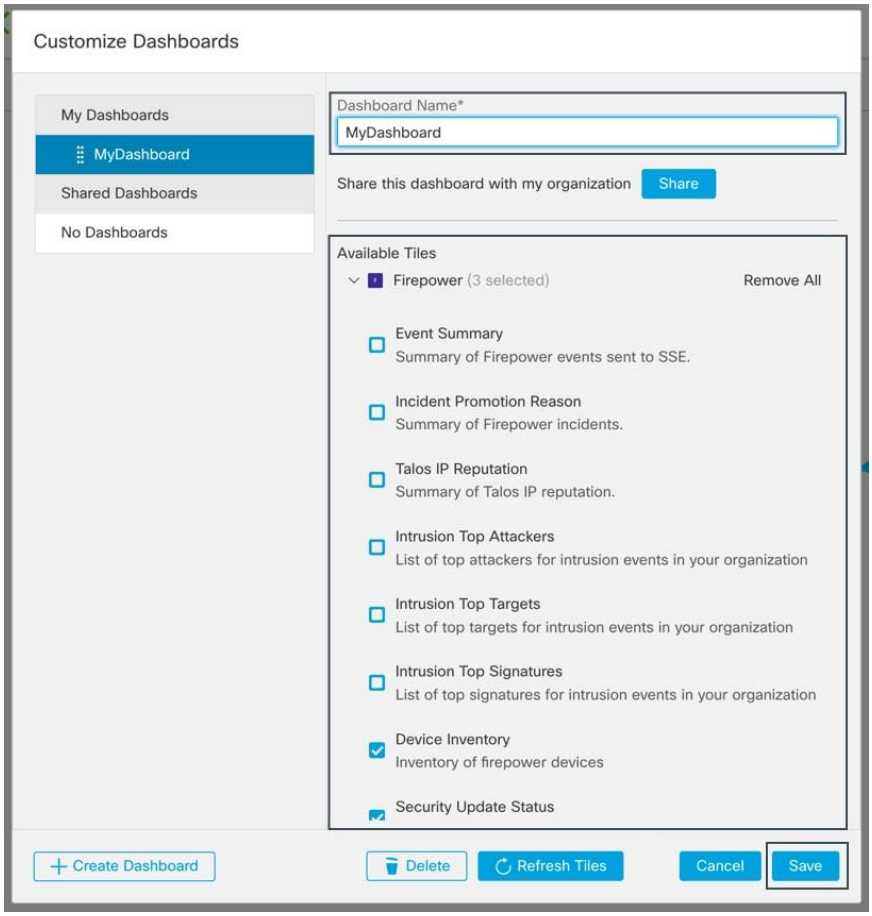

Рис. 3.23. Нова інформаційна панель

Після додавання плиток ви можете змінити їх розмір і перемістити в потрібне місце на інформаційній панелі SecureX

3.2. Інтеграція SecureX з Threat Grid Cloud

Cisco Threat Grid — це розширена автоматизована платформа для аналізу зловмисного програмного забезпечення та виявлення загроз, на якій підозрілі файли чи веб-адреси можуть бути виявленні та знешкодженні без впливу на середовище корпоративної мережі.

В інтеграції з SecureX Threat Grid є довідковим модулем і надає можливість переходу на портал Threat Grid для збору додаткової інформації про хеші файлів, IP-адреси, домени та URL-адреси в сховищі знань Threat Grid.

Процедура налаштування порталу Threat Grid – авторизуйте Threat Grid і отримайте ключ API:

1. Увійти у систему Threat Grid, використовуючи облікові дані адміністратора.

2. Перейти до розділу «Мій обліковий запис», як показано на рисунку 3.24.

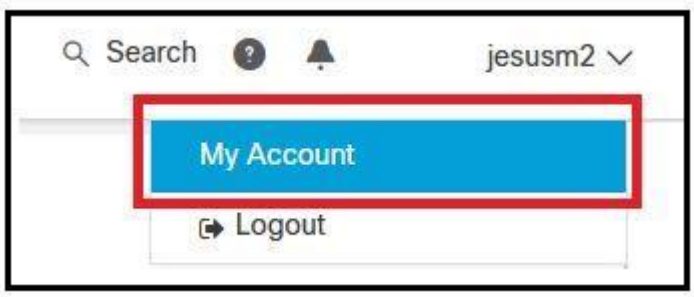

Рис. 3.24. Мій обліковий запис

3. Перейти до розділу «Підключення» та обрати параметр «Підключити відповідь на загрозу».

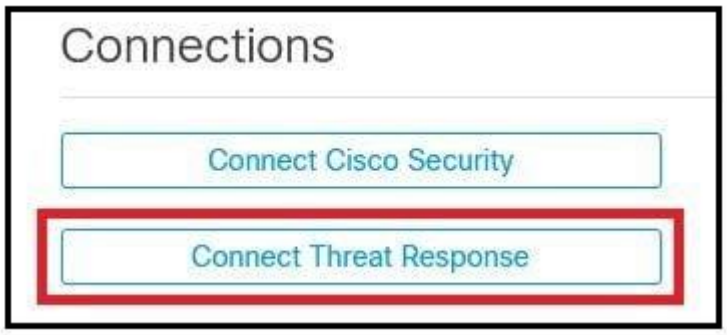

Рис. 3.25. Підключення відповіді на загрози

4. Обрати параметр «Авторизувати», щоб дозволити Threat Grid отримати доступ до Threat Response, як показано на рис.3.26.

Рис. 3.26. Авторизація Threat Grid

5. З'являється повідомлення «Авторизований доступ», щоб підтвердити, що Threat Grid має доступ до аналізу загроз і можливостей збагачення Threat Response.

6. Перейти до «Мій обліковий запис» -> «API» -> «Ключ API», скопіювати ключ API.

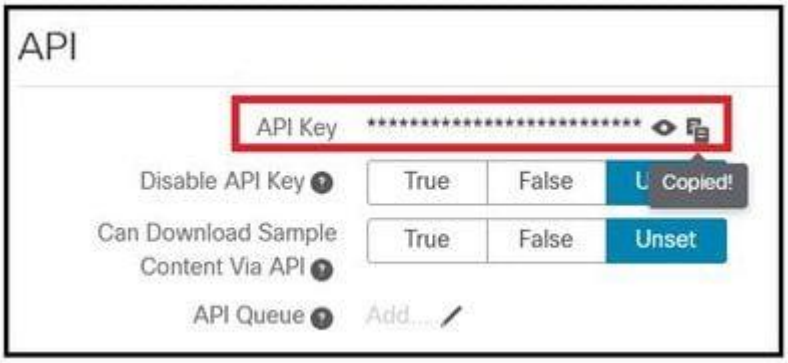

Рис. 3.27. Ключ API

Процедура налаштування порталу SecureX — налаштування модуля сітки загроз:

1. Увійти до SecureX, скористатися обліковими даними адміністратора.

2. Перейти на вкладку «Інтеграції», вибрати «Інтеграції» -> «Додати новий модуль»

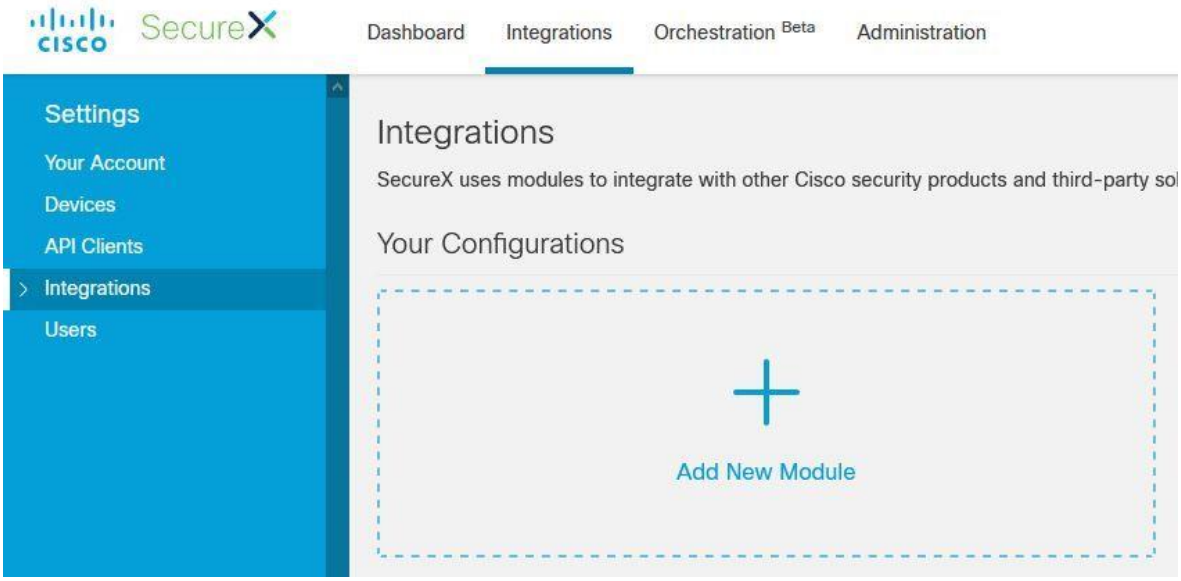

Рис. 3.28. Додавання нового модулю

3. На сторінці «Інтеграція» обрати «Додати новий модуль» на панелі модуля «Сітка загроз»

Рис. 3.29. Додавання новго модулю Threat Grid

4. Відкриється форма «Додати новий модуль». Необхідно заповнити форму та обрати «Зберегти», щоб завершити налаштування модуля Threat Grid.

- Назва модуля – залишити назву за замовчуванням або ввести ім’я, яке має значення для компанії.
- URL-адреса. З випадаючого списку обрати відповідну URL-адресу для розташування корпоративного облікового запису Threat Grid (Північна Америка чи Європа).
- Ключ API – ключ API сітки загроз (скопіювати та вставити ключ API зі сторінки TG).

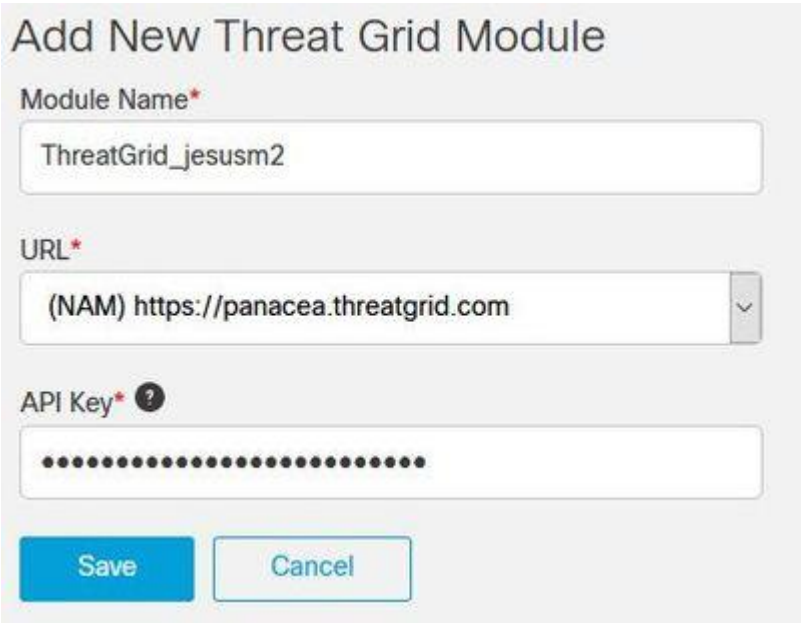

Рис. 3.30. Завершення додавання нового модулю

5. Тепер під копроративними конфігураціями на сторінці інтеграцій відображається сітка загроз

Процедура налаштування порталу SecureX - додати інформаційну панель сітки загроз:

1. На головній сторінці SecureX обрати +Нова інформаційна панель.

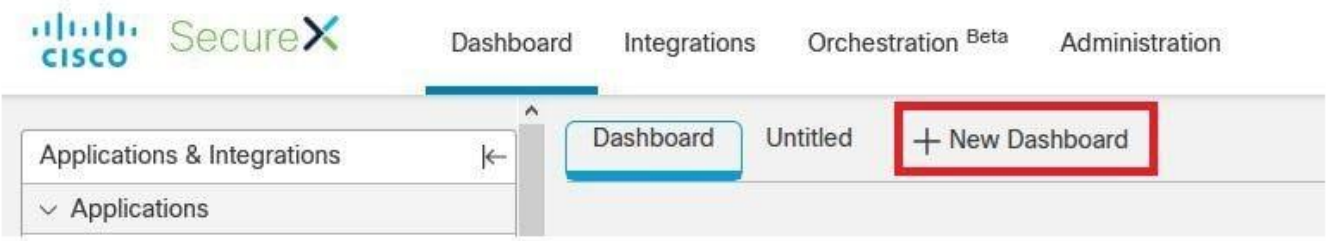

Рис. 3.31. Додавання нової інформаційної панелі

2. Обрати корпоративний модуль Threat Grid.

Рис. 3.32. Обрати створений модуль Threat Grid

3. Встановити назву інформаційної панелі.

4. Позначити параметри відповідно до корпоративних вимог і натиснути «Зберегти».

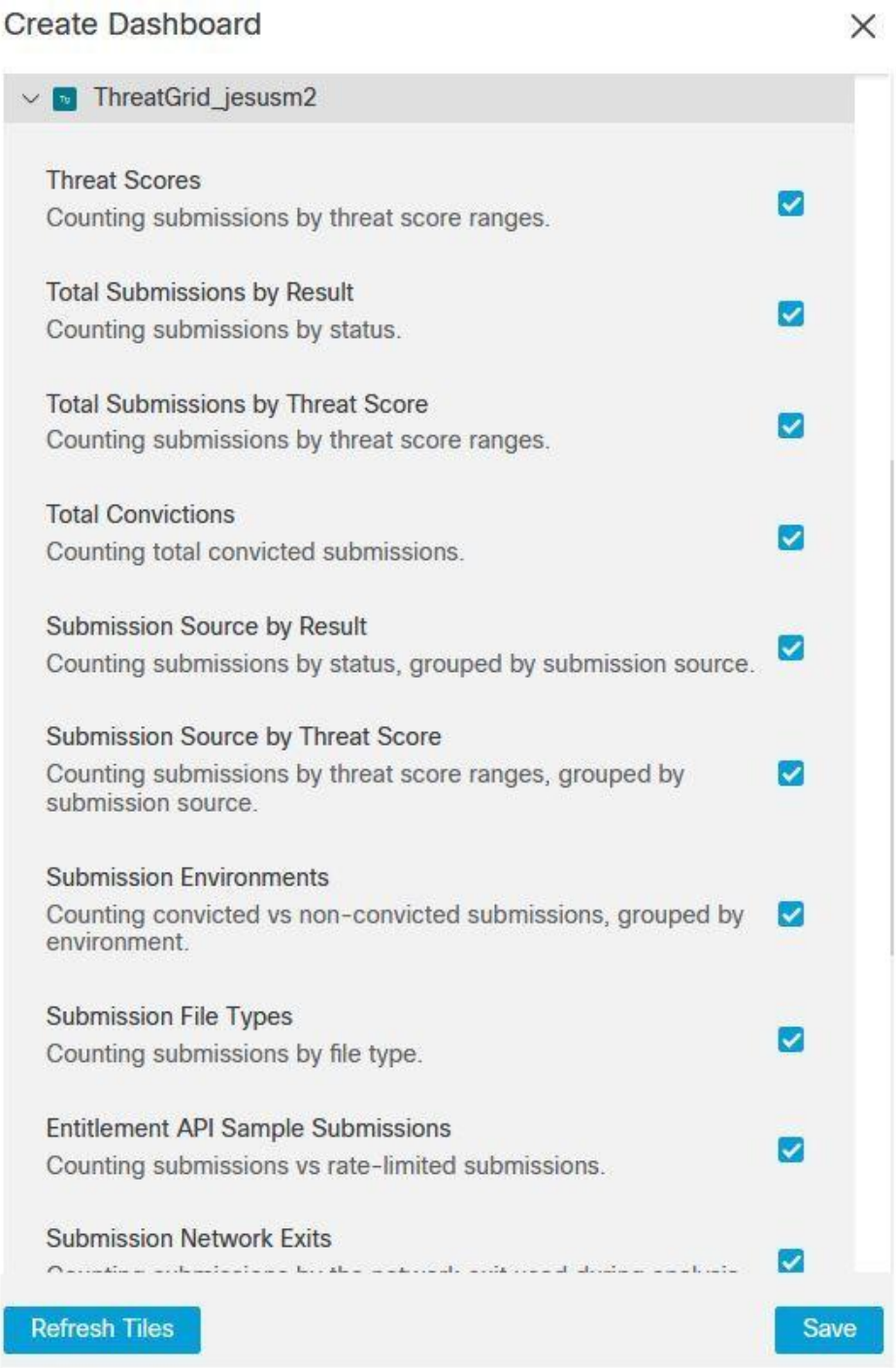

Рис. 3.33. Вибір необхідних параметрів

5. Можливо переглянути інформацію про сітку загроз на інформаційній панелі SecureX. Деталі, які відображаються на інформаційній панелі SecureX, надходять безпосередньо з інформаційної панелі Threat Grid, як показано на рис.3.34.

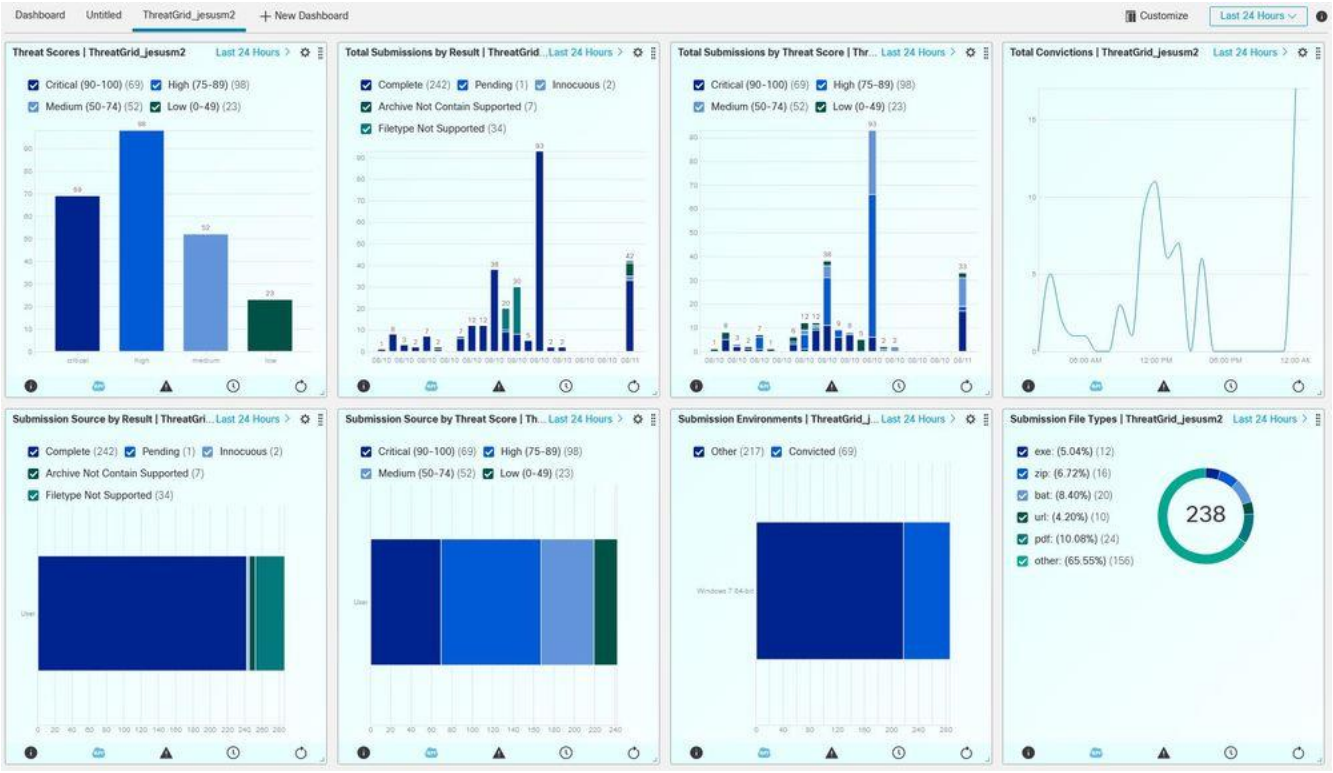

Рис. 3.34. Інформаційна панель Threat Grid

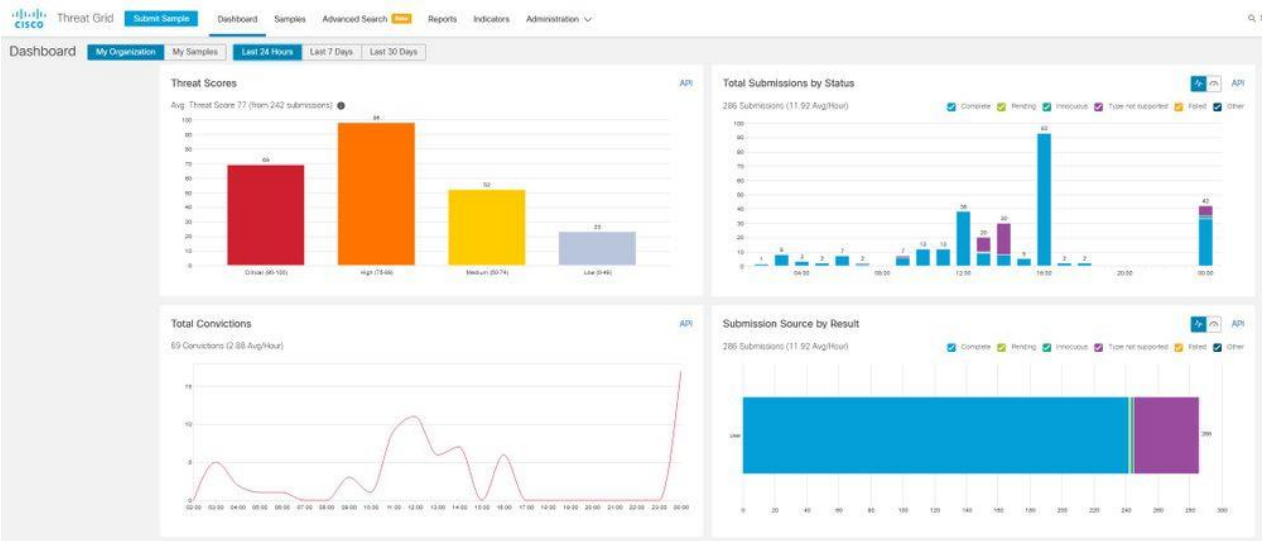

Рис. 3.35. Інформаційна панель SecureX

Процес налаштування розслідування реагування на загрози:

1. Перейти до порталу SecureX -> Applications & Integrations -> Threat Response і обрати Launch.

Рис. 3.36. Панель завантаження Threat Response

2. Він автоматично перенаправляє на портал Cisco Threat Response.

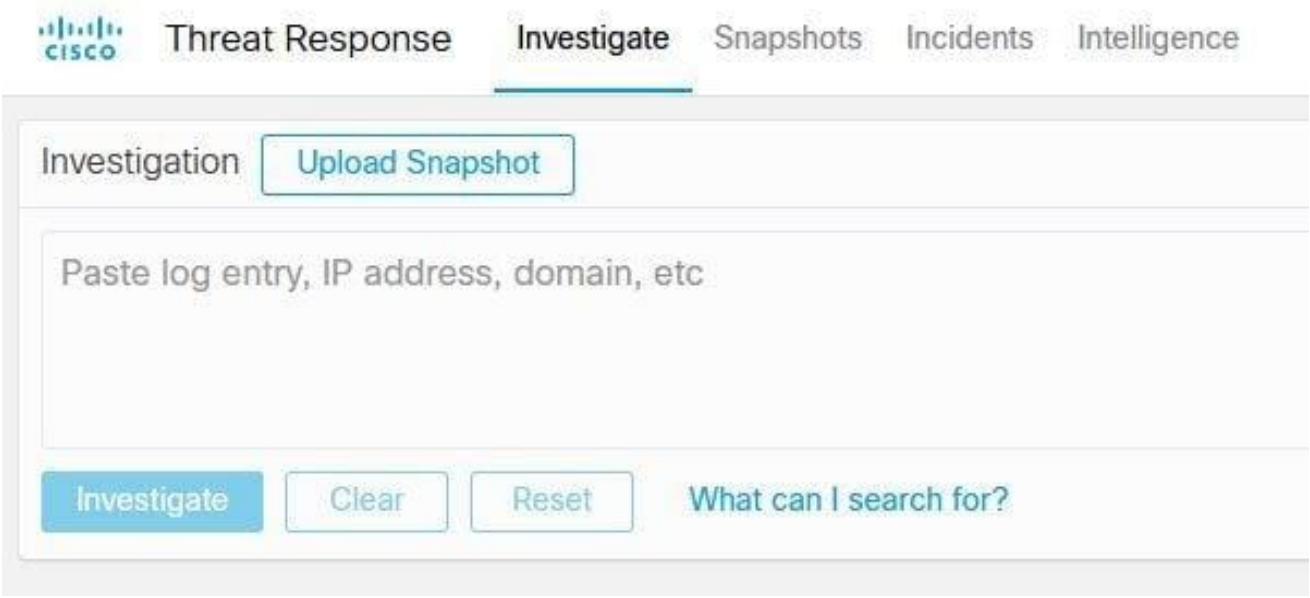

Рис. 3.37. Портал Cisco Threat Response

3. Можливо виконати дослідження на порталі Threat Response.

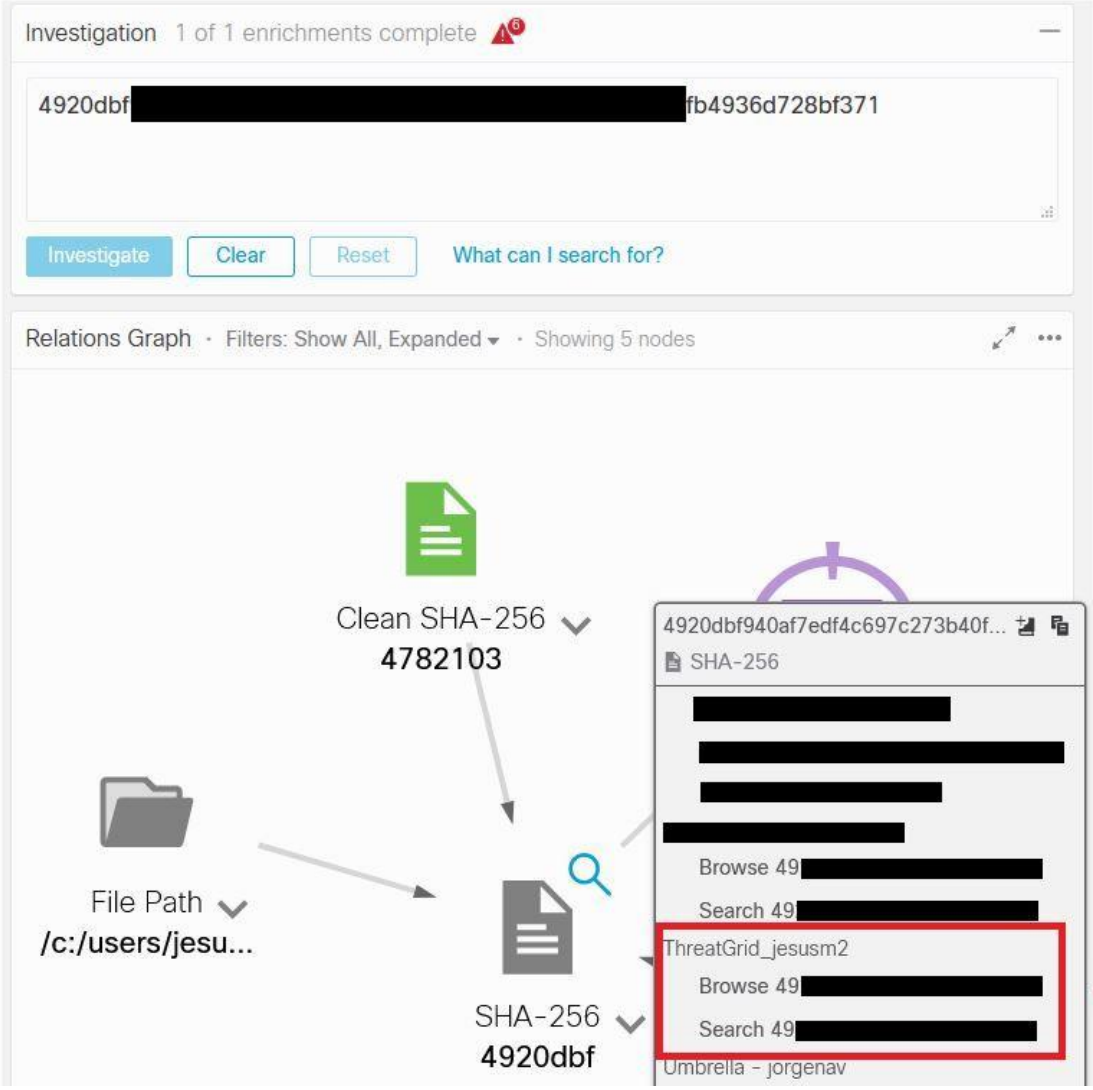

Рис. 3.38. Дослідження на порталі Threat Response

4. Можливо вибрати параметр «Огляд» або «Пошук». Він переспрямовує на портал Threat Grid для збору додаткової інформації про файли/хеші/IP-адреси/домени/URL-адреси в сховищі знань Threat Grid, як показано на рисунку 3.39.

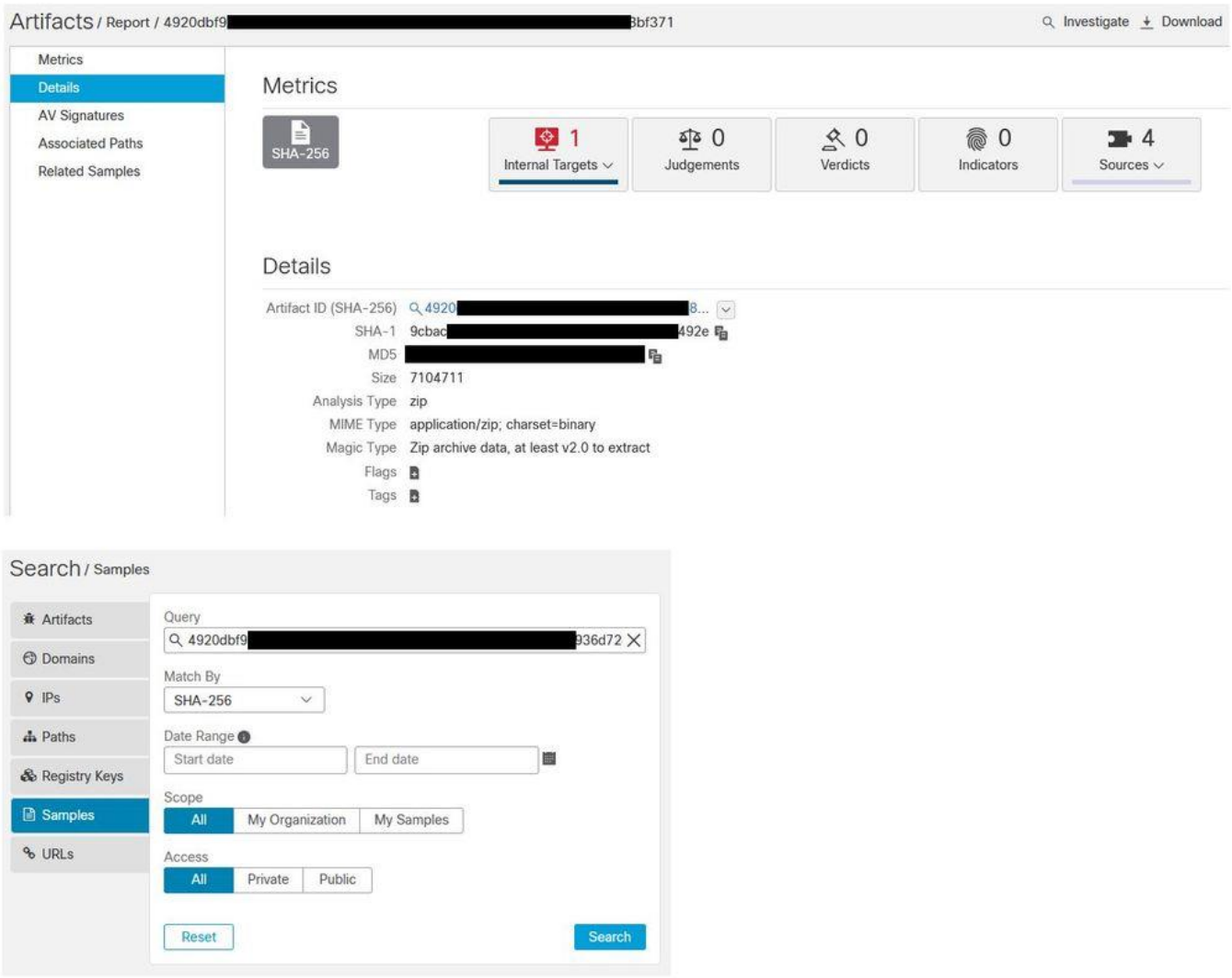

Рис. 3.39. Сховище знань Threat Grid

Усунення несправностей:

- Необхідно переконатися, що є обліковий запис користувача з правами адміністратора на TG, реагуванні на загрози SecureX і порталі SecureX.
- Переконайтеся, що наданий доступ до Connect Threat Response.
- Видалити старий модуль і створити новий модуль TG.

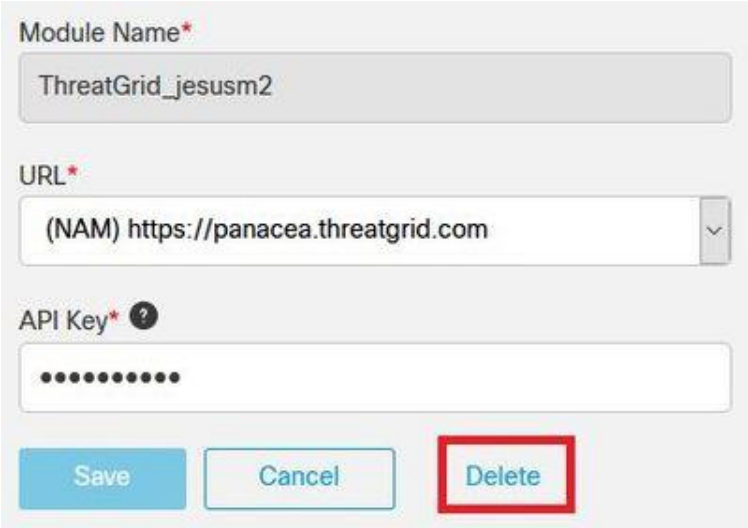

Рис. 3.40. Видалення старого модуля

- Необхідно переконатися, що позначку часу на порталі SecureX правильно встановлено.

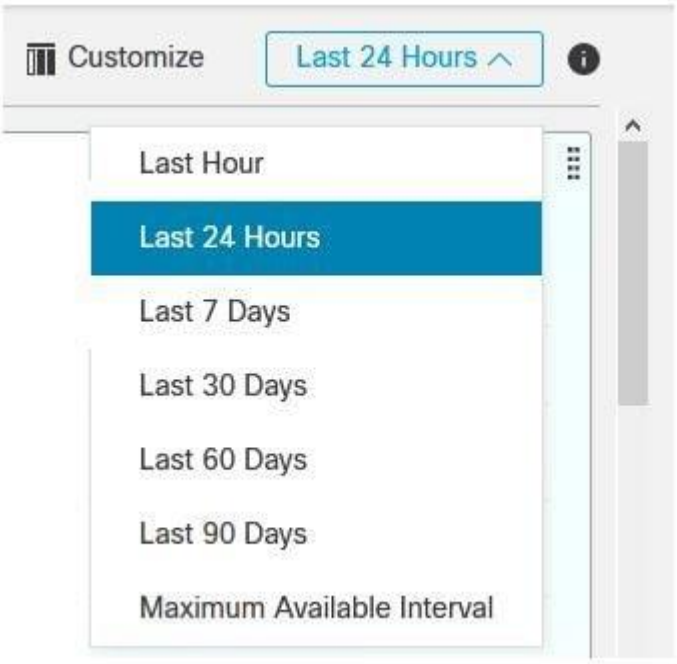

Рис. 3.41. Вибір коректної позначки часу

3.3. Інтеграція SecureX з Orbital Advanced Search

Orbital — це розширена функція Cisco AMP for Endpoints, призначена для спрощення дослідження безпеки та виявлення загроз. Вона забезпечує реалізацію потужної технології Osquery на кожній корпоративній кінцевій точці AMP. Orbital

дозволяє створювати власні запити для пошуку інформації, а також поставляється з понад сотнею попередньо готових запитів, які дозволяють швидко виконувати складні запити на будь-якій або всіх кінцевих точках.

Модуль Orbital має 4 плитки, які можна додати на інформаційну панель SecureX:

- Статистика запитів організації та результатів: набір показників, що описує запити та результати організації
- Статистика каталогу користувача: набір показників, який описує запити каталогу, які найчастіше використовуються цим користувачем.
- Статистика каталогу організації: набір показників, який описує запити каталогу, які найчастіше використовуються для цієї організації
- Статистика запитів і результатів користувача: набір показників, що описує запити та результати користувачів

Процедура налаштування:

1. Згенерувати облікові дані API в консолі SecureX:

- Увійти до SecureX
- Перейти до «Інтеграції» -> «Налаштування» -> «Клієнти API»
- Натиснути «Створити клієнт API» .
- Назвати клієнт, позначити Orbital, описати API та натисніть «Додати нового клієнта».

Рис. 3.42. Створення нового клієнта

- Облікові дані API генеруються

Рис. 3.43. Генерація облікових даних

2. Увімкнути стрічку SecureX у консолі AMP

SecureX — це централізована консоль і розподілений набір можливостей, які уніфікують видимість, забезпечують автоматизацію, прискорюють робочі процеси реагування на інциденти та покращують пошук загроз. Ці розподілені можливості представлені у вигляді додатків (додатків) та інструментів у стрічці SecureX, стрічку SecureX можна ввімкнути в Orbital Console:

- Увійти в Orbital Console
- На орбітальній консолі перейти до «Yout User» ->«Settings»
- Увімкнути стрічку SecureX
- Стрічка розташована в нижній частині сторінки та зберігається під час переходу між інформаційною панеллю та іншими продуктами безпеки у вашому середовищі

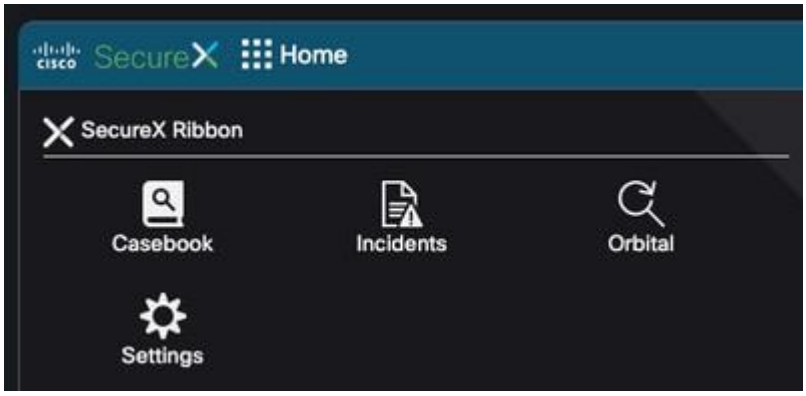

Рис. 3.44. Стрічка SecureX

3. Інтеграція Orbital Module у SecureX

Orbital може збагатити інформацію, представлену на графіку зв’язків Threat Response, якщо в Orbital надсилаються запити і збираються додаткові дані про хост, IP, IP4, IP6, MAC та ОС тощо. Програма Orbital доступна на стрічці SecureX і дозволяє виконати живий запит. Можливо переглянути показники та останні запити на правій панелі.

- На SecureX необхідно перейти до «Інтеграції» -> «Додати новий модуль»
- Обрати Orbital і натиснути «Додати новий модуль» .

- Назвати модуль і натиснути «Зберегти» .

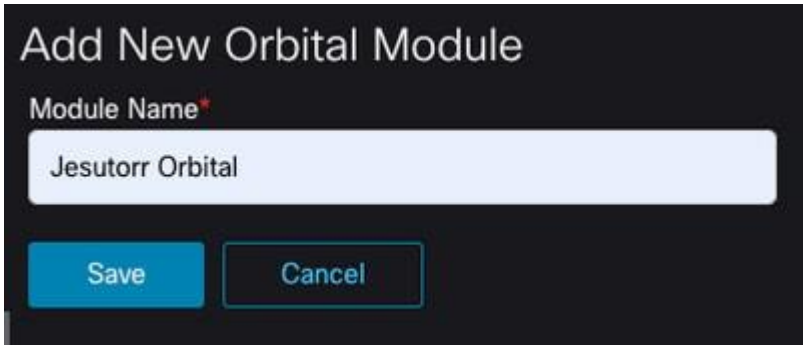

Рис. 3.45. Створення нового модулю

4. Підтвердження.

Необхідно переконатися, що інформація з Orbital Advanced Console відображається на інформаційній панелі SecureX:

- На SecureX перейти до панелі інструментів
- Натиснути «Нова інформаційна панель» і назвати її
- Вибрати раніше згенерований орбітальний модуль
- Обрати плитки та натиснути «Зберегти»

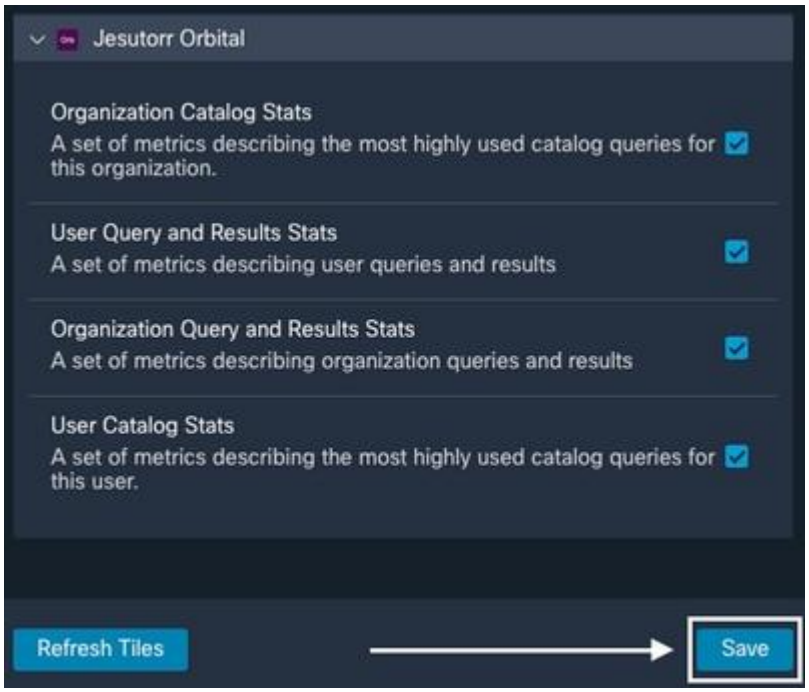

Рис. 3.46. Завершення інтегрування

- Обрати часові рамки та перевірити, чи дані з Orbital відображаються в SecureX

Розслідування можна почати зі стрічки SecureX

- Перейти до стрічки SecureX -> Orbital -> Perform an Orbital Query

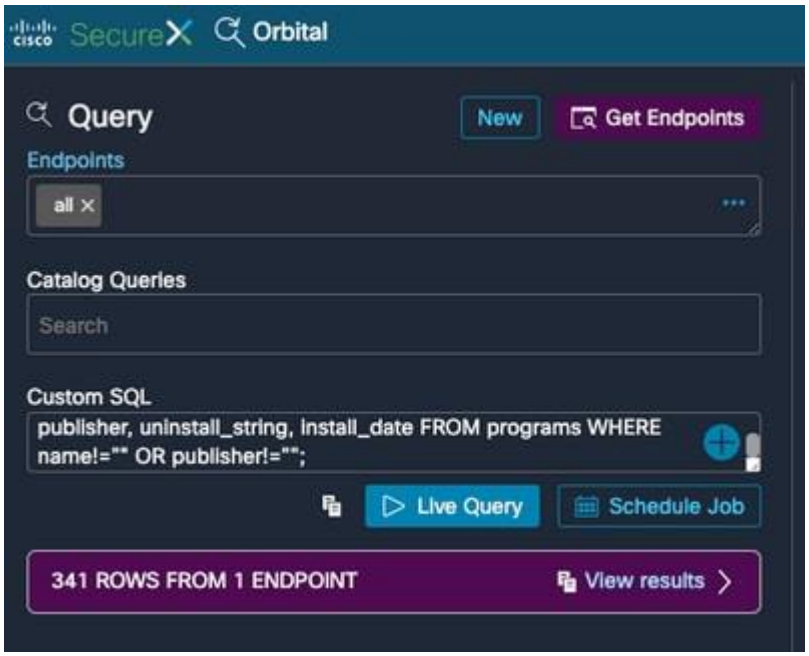

Рис. 3.47. Розслідування

Висновки до третього розділу

Досліджено методи та засоби забезпечення безпеки корпоративної мережі за допомогою рішення Cisco SecureX. Визначено та розглянуто три основні інтеграції - Cisco Secure Firewall Management Center, Threat Grid та Orbital Advanced, та наведено особливості їх роботи та підключення.

Підкреслено, що підключені інтеграції є дуже перспективними для використання в реальному часі корпоративною мережею, що суттєво спрощує роботу працівників для кожної проблемної області забезпечення безпеки роботи бізнес процесів.

ВИСНОВКИ

В магістерській роботі отримано наступні теоретичні та теоретично-практичні результати:

1. Розглянуто питання організації та забезпечення інформаційної безпеки в корпоративній мережі, були вивчені основні можливі загрози та вектори втрат даних для забезпечення безпеки бізнес процесів корпоративної мережі.

2. Проаналізовано ринок використання рішення, клієнти використовували ряд інструментів безпеки від Cisco та інших постачальників. Щоб дослідити та вирішити питання інформаційної безпеки до початку використання SecureX, команди що забезпечували безпеку бізнес процесів отримували прямий доступ до кожного з цих інструментів за допомогою різних інтерфейсів і паролів. Відсутність видимості та кореляції між цими інструментами призводила до того, що ріс ризик не помітити загрозу та погіршували швидкість і якість реагування на інциденти.

3. Зазначено, що після початку використання SecureX клієнти скоротили час аналітики на інцидент і отримали більше інформації про загрози безпеці в корпоративному середовищі.

4. Наведено та продемонстровано створення інтеграцій SecureX з такими продуктами як Cisco Secure Firewall Management Center, описано кроки для налаштувань модулів Orbital Advanced та Threat Grid.

5. Приділено увагу особливостям роботи інтегрованих продуктів та їх користь для забезпечення безпеки корпоративної мережі.