МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
Факультет комп'ютерних наук та технологій
Кафедра комп'ютерних інформаційних технологій

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач випускової кафедри
_____ Аліна САВЧЕНКО
«____»_____2023р

КВАЛІФІКАЦІЙНА РОБОТА

(ДИПЛОМНА РОБОТА, ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СПУПЕНЯ

"МАГІСТРА"

ЗА ОСВІТНЬО-ПРОФЕСІЙНОЮ ПРОГРАМОЮ «ІНФОРМАЦІЙНІ УПРАВЛЯЮЧІ СИСТЕМИ ТА ТЕХНОЛОГІЇ»

Тема: «Системи моніторингу та боротьби з кіберзагрозами на базі WSS, EDR та PAM рішень»

Виконавець: студент УС-211м СКРИПНІК Олександр Андрійович
(студент, група, призвіще, ім'я, по батькові)

Керівник: д.т.н., доцент САВЧЕНКО Аліна Станіславівна
(науковій ступень, вчене звання, призвіще, ім'я, по батькові)

Нормоконтролер: _____Ігор РАЙЧЕВ_____
(П.І.Б.) (підпис)

Київ - 2023

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет *Комп'ютерних наук та технологій*

Кафедра *Комп'ютерних інформаційних технологій*

Галузь знань, спеціальність, спеціалізація: 12 "Інформаційні технології", 122 "Комп'ютерні науки", "Інформаційні управляючі системи та технології"

ЗАТВЕРДЖУЮ
Завідувач кафедри
Аліна САВЧЕНКО
"_____"_____ 2023 р.

ЗАВДАННЯ

на виконання кваліфікаційної роботи студента

Скрипніка Олександра Андрійовича

(прізвище, ім'я, по батькові)

1.Тема роботи: «Системи моніторингу та боротьби з кіберзагрозами на базі WSS, EDR та PAM рішень» затверджена наказом ректора від "29" вересня 2023р. за №1976/ст

2. Термін виконання роботи: з 02 жовтня 2022р. по 31 грудня 2023 р.

3. Вихідні дані до роботи: аналіз сучасних векторів атак, інтеграція PAM (Fudo), WSS (Symantec), EDR (Fidelis).

4. Зміст пояснювальної записки (перелік питань, що підлягають розробці): вступ, аналітичний огляд і постановка задачі, огляд технологій та інструментів для розробки системи, розробка функціональності системи та інтерфейсу для користувачів, висновки.

5. Перелік обов'язкового графічного матеріалу: схема інтеграції рішення в IT-системі підприємства.

6. Календарний план-графік

№ з/п	Етапи виконання дипломної роботи	Термін виконання етапів	Примітка
1	Аналіз літератури та джерел за темою дипломного проекту.	01.10.2023-05.10.2023	
2	Розробка та затвердження плану дипломного проекту.	10.10.2023-13.10.2023	
3	Проведення консультації з науковим керівником щодо створення першого розділ.	14.10.2023-20.10.2023	
4	Аналітичний огляд і постановка задачі.	23.10.2023-15.10.2023	
5	Порівняльний аналіз існуючих систем управління документами.	28.10.2023-30.10.2023	
6	Огляд технологій для розробки системи.	01.11.2023-05.11.2023	
7	Розробка компонентів системи.	08.11.2023-12.11.2023	
8	Висновки та оформлення пояснювальної записки дипломного проекту.	15.11.2023-20.11.2023	
9	Підписання необхідних документів у встановленому порядку.	22.12.2023-25.12.2023	
10	Підготовка до захисту та попередній захист дипломного проекту на випусковій кафедрі дипломного проекту	22.12.2023-24.12.2023	

7. Дата видачі завдання: «02» жовтня 2023 р.

Керівник дипломного проекту _____ Аліна САВЧЕНКО
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Олександр СКРИПНИК

(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Пояснювальна записка до дипломного проекту «Системи моніторингу та боротьби з кіберзагрозами на базі WSS, EDR та PAM рішень» викладена на 87 сторінках і містить 58 рисунків, 10 наукових джерел.

Об'єкт дослідження: процес інформаційного обміну в організації.

Предмет дослідження: методи керування інформаційною безпекою, сучасні методи атак та інструменти боротьби з вразливостями.

Мета роботи: підвищення рівня інформаційної безпеки організації за рахунок системи моніторингу та боротьби з кіберзагрозами із застосуванням керування привілейованим доступом (PAM) Fudo, виявлення вразливостей цілеспрямованих атак (EDR) Fidelis, системи безпеки веб додатків (WSS) Symantec.

Методи дослідження, аналіз літературних джерел, порівняльний аналіз, технічні та програмні засоби: аналітика, розробка бази даних за допомогою MySQL, розробка кастомних скриптів для написання певних правил, обробка літературних джерел.

Отримані результати та їх новизна: проведено огляд сучасних методів атак та протидії їм, кастомізація інструментів для виявлення новітніх типів вразливостей, проаналізовано новітні вектори атак на кінцеві цільові системи, розглянуто можливості адміністрування рішень для протидії зазначеним видам загроз, розроблено системи моніторингу та боротьби з кіберзагрозами.

Ключові слова: УПРАВЛІННЯ СИСТЕМАМИ ПРИВІЛЕЙОВАНОГО ДОСТУПУ ДО ЦІЛЬОВИХ СИСТЕМ, БАЗИ ДАНИХ, РОБОЧИЙ ПРОЦЕС, SQL, PYTHON, SYMANTEC, FUDO, FIDELIS.

ЗМІСТ

ВСТУП

На сьогоднішній день пріоритетною задачею кожного підприємства є захист даних свої замовників та працівників. Аналізуючи тенденцію розвитку нових векторів атак, можна зробити висновок, що вони стають більш складними для виявлення та потребують час від часу залучення допоміжних осіб для реалізації поставленої цілі.

Якщо переглядати надану статистику, яку надає Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA, було зареєстровано та опрацьовано близько 100 тисяч кіберінцидентів, більшість з них – поширення шкідливого програмного забезпечення та фішинг. Отже, найчастіше зловмисники використовують такі методи атак, як Фішинг, СМІшинг, Malicious.

Згідно цієї статистики можна зробити висновок, що Україна є ціллю на, яку спрямовують різні види та тактики атак для заподіянню шкоди IT-інфраструктурі держави.

На даний час є загроза не лише IT-інфраструктурі та Internet of Things (IoT), тобто є необхідність враховувати це при проектуванні захисту мережі. Це є критично важливим, оскільки обрана стратегія захисту, має на меті використання стороннього допоміжного програмного комплексу (агенту). В такому випадку буде здійснювати збирання даних для аналізу та розслідування інцидентів, а також реагування на них. В IT-інфраструктурі пристрої обмінюються інформацією за допомогою певних протоколів, наприклад, стандартні протоколи SSH, WMI тощо. В IoT використовуються так звані пропрієтарні протоколи, які система захисту повинна відслідковувати та відповідно реагувати.

На сьогодні необхідним є також зменшення документообігу всередині організації та розмежування прав доступу користувачів до кінцевих цільових систем, наприклад, робочих станцій, веб-ресурсів, серверної інфраструктури. Коли потрібно отримати корпоративний доступ до певної інформаційної

системи компанії, користувачу необхідно здійснити ряд запитів у вигляді листів на ім’я адміністратора, який, в свою чергу, має отримати погодження зі своїм керівником. Це призводить до незручностей в роботі та втрати робочого часу працівника. Зазначені проблеми вирішує система керування привілейованим доступом користувачів, яка має на меті за допомогою вбудованої рольової моделі надавати доступ, користувачу, Користувач, який не мав можливості мати безперервний доступ до певної цільової системи може отримати її за допомогою запиту в середині програмного рішення, що замінює лист з вимогою про надання доступу. Якщо користувач виконає не легітимні дії, які призведуть до порушення роботи системи, це буде задетиктовано та сформовано звіт на вимогу адміністратора. Отже така система сприяє не лише зменшенню документообігу, а й підвищенню контролю і спрацювання на певні дії користувача, в тому числі повна відео фіксація його дій під час роботи з системою.

Інструменти, які будуть використані під час даної роботи, - це програмні комплекси, що забезпечують захист внутрішнього периметру організації, де вони використовуються. Але це не гарантує повного захисту системи, тому що дані системи постійно потребують оновлення правил, які будуть спрацьовувати вразі виявлення певних порушень в системі.

Якщо дивитися в розрізі розгортання даних програмних комплексів, то більшість користувачів згідно аналізу віддають перевагу віртуальному середовищу такому, як VmWare, HyperView. Дані механізми дають змогу легко здійснювати масштабування даних рішень в форматі побудови відмовостійких кластерів. Деякі програмні комплекси, що є досить популярним представлені в хмарному середовищі та надаються вендорами, як тенанти.

Дивлячись на тенденцію сьогоднішнього часу, а саме мова йде про Україну, більшість користувачів здійснили міграцію своєї інфраструктури в хмарне середовище наприклад GoogleCloud, Aws, Azure, CloudFlare. Це дає їм можливість захистити свою інфраструктуру від такого типу атак, як

Dos/DDos. Однак є необхідність розгортання додаткових механізмів захисту в даних середовищах. Тому при побудові тактики захисту інфраструктури потрібно проводити глибокий аналіз та обирати оптимальний метод захисту системи.

Тому метою роботи є підвищення рівня інформаційної безпеки організації за рахунок системи моніторингу та боротьби з кіберзагрозами із застосуванням керування привілейованим доступом (PAM) Fudo, виявлення вразливостей цілеспрямованих атак (EDR) Fidelis, системи безпеки веб додатків (WSS) Symantec.

Об’єкт дослідження є процес інформаційного обміну в організації

Предмет дослідження методи керування інформаційною безпекою, сучасні методи атак та інструменти боротьби з вразливостями,

Задачі, які потрібно вирішити це провести аналіз мережі на підприємстві, знайти слабкі сторони, та розробити системи, які здійснять повноцінний захист мережі організації.

РОЗДІЛ 1
АНАЛІТИЧНИЙ ОГЛЯД І ПОСТАНОВКА ЗАДАЧІ

На даний момент існує безліч вразливостей для інформаційних систем, які спроможні завдати нищівного удару по інфраструктурі підприємства, яка за собою спровокує, як матеріальні затрати так і репутаційні. З кожним днем методи атак, які спрямовуються на організації стають більш складнішими для виявлення стандартними інструментами моніторингу та швидкого реагування на них без участі оператора системи. Тому захист інформаційної системи – це застосування комплексних рішень, які спрямовані для мінімізації ризиків проникнення зловмисників на внутрішній периметр організації, що ставить на своїй меті забезпечити виявлення аномальної активності в середині організації на початкових стадіях.

1.1. Методика проведення атаки

Перед тим, як здійснити атаку, зловмисник проводить аналіз системи, розвідку, і головне вже на цьому етапі потрібно його вирахувати та прийняти дії проти подальшої ескалації. Досить вдало це ілюстровано на дані схемі, як побудована атака рис 1.1.

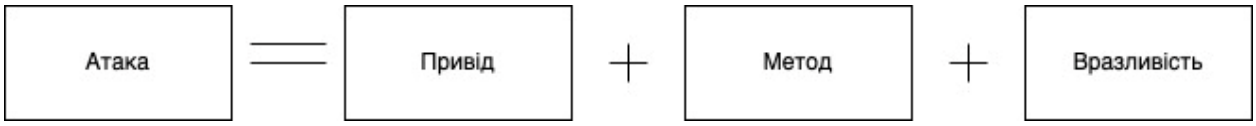

Рис.1.1. Схема побудови атаки

З даної схеми видно, що привід з’явиться тоді, коли зловмисник буде розуміти, що система проти якої буде спрямовано його активність, буде мати

в собі критично важливу (чуттєву) інформацію. Методи - це те як буде відбуватися атака проти цільової системи. Вразливість - це виявлена зловмисником слабке місце системи на початковому етапі за допомогою аналітичної діяльності спрямованої проти системи. З цього можна зрозуміти що перед тим, як почати активні дії зловмисник буде проводити розвідку, для виявлення слабкого місця.

Атаки можна класифікувати згідно центру міжнародної системи специфікації IATF, яка виокремлює 5 категорій [1]:

1. Пасивні – це є аналіз на основі перехоплення мережевого трафіку цільової системи. Даний тип атаки проводиться за допомогою сніферів, тому що є змога за допомогою цих інструментів отримати дані у не зашифрованому вигляді наприклад облікові данні або відкритий текст.
2. Активні атаки – застосовуються з ціллю виведення з ладу системи з робочого стану, шляхом відправки активного трафіку великого обсягу, який може спричинити перевантаження.
3. Атаки з ближньої відстані – даний тип атаки, також носить назву соціальна інженерія, яка спрямована на близький контакт з цільовою системою шляхом маючи доступ через людський фактор.
4. Інсайдерська атака – даний тип атаки виконується довірливим лицем.
5. Розповсюджуюча атака – даний тип атаки побудований на так, що зловмисник вбудовує в операційну систему вже вбудований скрипт, який буде спрямований на здійснення подальших нелегітимних дій у системі, при встановленні даного програмного забезпечення звичайним користувачем, та може розповсюджуватися в середині мережі та оновлюватися якщо дана система матиме вихід в Інтернет.

1.2. Аналіз вразливостей в інформаційній безпеці організації

В даний момент, найбільш розповсюджені атаки це DDos. Даний тип атак з кожним днем стає більш небезпечним, тому що Атака типу «відмова в обслуговуванні» Dos, та «розподілена відмова обслуговуванні» DDos, націлені на те щоб цільова система (робоча станція, мережевий ресурс) стала недоступною для авторизованих користувачів.

Наступний тип атаки, який досить розповсюджений, фішинг займає за статистикою друге місце з найчастіше використовуваних атаках на цільові системи. Даний тип атаки побудований на соціальній інженерії тому, що ціль фішингової атаки є спровокувати жертву перейти або відкрити вкладення електронного листа. Тобто Фішинг – це метод атаки, при якому зловмисник відправляє електронний лист або надає посилання яка буде імітувати присутність користувача на законному ресурсі або інформацію про обліковий запис. Зловмисник реєструє підробне доменне ім’я та створює підробний веб-ресурс а після чого здійснює надсилання посилання через пошту до користувача. Після чого потенційна жертва здійснює перехід по скомпрометованому посиланню, яке перенаправляє користувача на підробний веб-ресурс на якому його будуть змушувати поділитися власними персональними даними. Але даний тип атак націлений на необізнаних користувачів які можуть не помітити те що даний ресурс на який їх переадресоване посилання буде нелігітимним.

Зазвичай дані типи атак використовують вразливості протоколів моделі TCP/IP або якщо існують конкретні вразливості в операційній системі (ОС).

Суть цього вектору атак побудовано на тому, щоб направити на цільову систему користувача незаконні запити або трафік з ціллю перевантажити її ресурси та довести до недоступності ресурсу на який здійснюється дана атака.

Ціль даної типу атак не отримати несанкціонований доступ до системи або пошкодити дані, а забезпечити недоступність ресурсу авторизованими користувачами.

Сьогодні зловмисники часто застосовують такий метод атаки, як Руткіти — це програми, призначені для отримання доступу до комп'ютера без виявлення.

Програмне забезпечення (ПЗ) націлене на полегшення отримання несанкціонованого доступу до віддаленої системи та виконння дії, яка буде направлена на заволодіння чи виведення з ладу IT-інфраструктури цільової організації.

Метою руткіта є отримання привілеїв root для системи.

Сьогодні більшість користувачів головною задачею визначають захист інформаційної системи шляхом впровадженням, мінімізації ризиків та здійснення аналітики в реальному часі, щоб реагувати на різноманітні події в системі.

Як приклад розглянемо атаку, спрямовану на електронний ресурс організації. Всі дії в даній роботі виконуються на віртуальних машинах та не наносять шкоді реальним системам.

Кожна організація має адміністративний портал за допомогою, якого здійснюються певні дії наприклад, в банківському секторі. За допомогою даного порталу є можливість здійснювати доступу до БД клієнтів та до різних рахунків та здійснювати управління ними.

Дана атака буде проведена за допомогою інструменту « Gobuster».

« Gobuster» - це є популярний інструмент для брут-форсингу. В даному застосунку застосовується метод брут-форсу, що здійснює автоматизований підбір пароля за допомогою виконання математичних операції, а також за допомогою словника, в якому зібрані базові шаблони, які використовують користувачі і дані словники поповнюються новими паролями, які були отримані несанкціонованим способом.[2]

Інструмент виконує такі функції:

- URI (директорій та файлів) у веб-сайтах;
- DNS субдоменів (за допомогою підстановочних символів);
- Імен віртуальних хостів на цільових веб-серверах.

Це інструмент командного рядка, написаний на Go, він не виконує рекурсивний брут-форс, дозволяє одночасно брут-форсити папки та кілька розширень, компілюється на безлічі платформ, працює швидше за інтерпретовані скрипти (такі як Python), не вимагає середовище виконання.

Для прикладу використовується операційна система «Ubuntu».

Вводимо наступну команду в термінал, щоб знайти потенційно приховані сторінки на веб-сайті FakeBank за допомогою GoBuster (додаток безпеки командного рядка).

gobuster -u http://fakebank.com -w wordlist.txt dir

На рис.1.2, можна побачити, що GoBuster сканує веб-сайт за кожним словом у списку, знаходячи сторінки на сайті. GoBuster повідомить вам сторінки, які він знайшов у списку імен сторінок/каталогів (позначається статусом: 200).

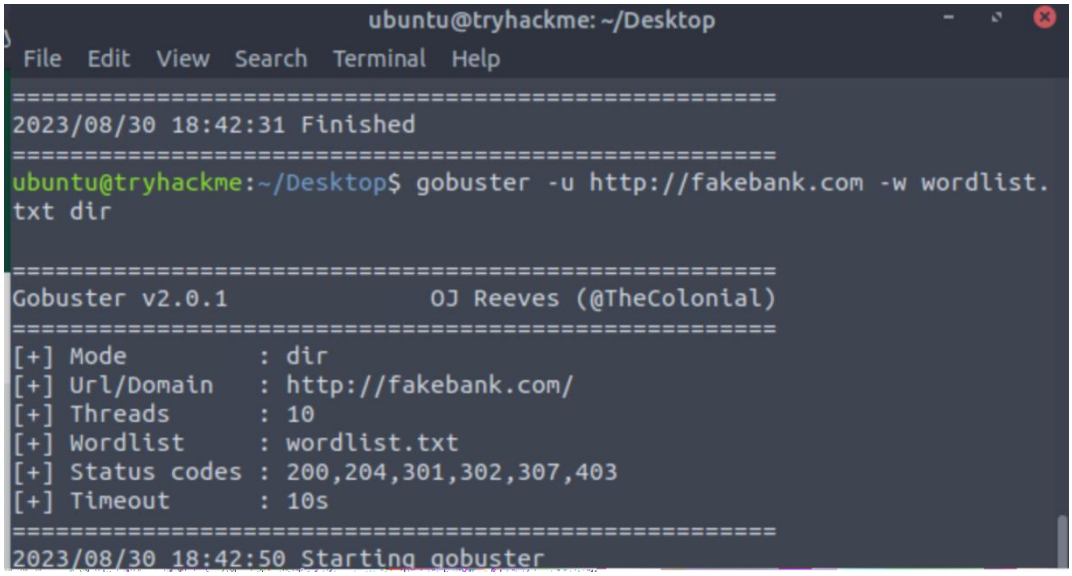

Рис. 1.2. Сканування веб-сайту

З даної інформації, яку бачимо на зображені, залишається перейти за посиланням: *fakebank/bank-transfer*. З даної сторінки, є можливість вже здійснювати транзакції на різні рахунки.

Якщо б в даній організації була б реалізована система EDR або XDR, за допомогою, якої можна було б отримати інформацію про мережеву активність на основі копії трафіку. Після чого, якщо була здійснена нелегітимна активність, система спрацювала спочатку направивши «Alert» в систему та на пошту адміністратора системи за допомогою інтеграції з поштовим сервісом. Якщо рішення є активним, а не пасивним була би прийнята дія на основі написаних «Yara» правил, які блокують виконання даної дії збоку зловмисника. Навіть за допомогою даних рішень можна заблокувати фішингові листи, тому що є механізм, який аналізує пошту та направляє листи в ізольоване середовище «sandbox» для детального аналізу та визначення звідки була здійснена відправка листа. Головною особливістю цих рішень є також повний контроль кінцевих цільових систем користувачів, на яких встановлюється «агент», який здійснює повний моніторинг системи та перешкоджає запуску сторонніх процесів з робочих станцій користувачів, якщо був отриманий несанкціонований доступ до них.

Навіть за умов, якщо в системі організації, буде встановлене примітивне рішення «PAM», що здійснює контроль за доступом привілейованих користувачів до цільових систем. За допомогою цього рішення можна закрити ряд проблем пов’язаних з моніторингом, доступом користувачів до цільових систем. Тобто користувач, коли буде здійснювати підключення до цільової системи буде здійснювати запис повної активності користувача, а також детекцію за допомогою «keystroke» та спрацювання на них прописаних правил, та запис повної активності користувача за допомогою відео, що дасть змогу здійснити перегляд та аналіз дій користувача. На додаток користувач при підключені не вводить облікові данні від системи, а лише від «PAM», здійснює «прокидання» облікових даних, що робить неможливим в підборі паролю, якщо користувач його розкрив. Навіть якщо це буде здійснено, є можливість налаштувати запит на підключення шляхом погодженням від адміністратора «PAM».

Вище описані проблеми та вразливості, можна вирішити, за допомогою рішень PAM, WSS, EDR. Дані рішення мають можливість аналізувати трафік, як в середині організації так і за її межами.

1.3. Огляд системи на Fudo PAM

Продукт Fudo PAM, на сьогоднішній день є досить часто інтегрованим рішення в інформаційну систему підприємства. Дане рішення входить в сімейство рішень, які відповідають за контроль привілейованого доступу користувачів, та відповідає за контрольоване управління користувацькими сесіями з можливістю отримання контролю над активним сеансом.

Головна проблема, з якою стикаються більшість підприємств, тещо вирішує дане рішення це тещо сьогодні більшість користувачів здійснюють управління своєю інфраструктурою в тому числі безпековою у віддаленому режимі за допомогою VPN-агентів, в деяких випадках використовуються міжмережеві екрани, головна ціль яких це розділення доступу в корпоративну мережу. По суті можна зафіксувати лише факти створення VPN-з'єднання, доступу до одного з цільових ресурсів у певний момент часу та закінчення роботи з ним. При необхідності деталізації сеансу та аналізу конкретних дій, які робив користувач, офіцери безпеки часто залишаються «сліпими». Величезний арсенал засобів безпеки, які представлені на ринку, спрямований на захист того, що розміщується до цільового ресурсу або конкретної програми. Однак лише деякі з інструментів можуть дати нам відповідь про те, що робить користувач за тими «дверима», куди ми його все ж таки допустили. Окремий пласт проблем відноситься до наявності знеособлених облікових записів з привілеями суперкористувача, а також до облікових записів топ-менеджменту компанії. За умовчанням вони сприймаються системами безпеки як довірені та будуть безперешкодно допущені до необхідних ресурсів. Такі облікові записи є бажаною метою для

кіберзлочинців, а й, що менш важливо, створюють численні змогу зловживань всередині організації.

PAM системи, в тому числа рішення Fudo Pam, дає можливість здійснити захист витоку конфіденційної інформації із-за дій користувача, які могли до цього призвести.

Досить часто в підприємствах, як приватного секторну так і державного є необхідність використання саме безагентського рішення. Тому що агент позиціонує, як додаткове стороннє програмне забезпечення, яке необхідно встановити на цільові системи з метою моніторингу. Також є досить проблематично, коли для роботи системи є необхідністю встановлення агента на робочу станцію користувача, тобто здійснення підключення буде відбуватися через встановлений агент.

Fudo PAM є повністю безагентським рішенням що здійснює контроль та моніторинг активності користувачів. Дане рішення працює на рівні протоколів, що дає можливість розбирати трафік, здійснювати індексацію та приймати оперативні дії, якщо буде спрацювання за регулярними виразами.[3]

Важливою особливістю Fudo PAM є зберігання відеозапису сеансу, а вихідного трафіку, на основі якого надалі можна відновити візуальну картину дій користувача. Окрім іншого, такий підхід суттєво знижує навантаження на інфраструктуру та дає можливість автоматично реагувати на дії користувача в режимі реального часу. Система створена на базі індивідуалізованого та повністю ізольованого ядра FreeBSD. Вибір платформи невипадковий: співзасновник та технічний директор компанії Fudo Security Павло Давидек є одним із ключових розробників FreeBSD. Функціональні можливості Fudo PAM можна умовно поділити на сім частин.

Система здійснює підтримку таких протоколів, як (HTTP, HTTPS, ICA, Modbus, SQL, MySQL, RDP, SSH, Telnet 3270, Telnet 5250, Telnet, VNC, X11, TCP), якщо є необхідність здійснювати підключення по іншому протоколу, який не підтримується нативно, є можливість використовувати технологію

джамп-хостів. Сесії, які записуються тобто є активними, можна переглядати, як у записі так і в live-режимі. В деяких протоколах можна здійснити підключення до активної сесії чи здійснити її розірвання.

Унікальною функцією системи є OCR-обробка сесій з розпізнаванням тексту та пошуком за ключовими словами та командами на семи мовах, включаючи Українську. Крім цього, аналіз трафіку «на льоту» дає можливість автоматично реагувати на дії користувача у разі виявлення ключових виразів, заданих у політиках безпеки. Завдяки технології OCR є можливість реагувати не тільки на команди і текстову інформацію, що вводяться, але також і на графічні заголовки інтерфейсних вікон (наприклад, якщо користувач навіщось звернувся до настройок засобів ІБ — клієнта EDR, DLP та ін.).[5]

В Fudo PAM, представлено дві консолі управління (адміністративна, користувацька).

Адміністративна консоль управління відповідає за повну, централізовану можливість здійснювати управління та адміністрування. За допомогою вбудованої рольової моделі, яка представлена в рішенні, до неї є доступ лише в (superadmin, admin, operator). Глобальні налаштування може здійснювати користувач з роллю superadmin, admin лише доступ до налаштування підключень, operator перегляд сесії та звітів.

Користувацька консоль відповідає за можливість здійснювати підключення користувачами до цільових систем з однієї консолі та здійснює завантаження нативних клієнтів для підключення в форматі стороннього клієнту.

1.4. Архітектура Fudo PAM

Fudo PAM здійснює обробку всього трафіку між користувачами не має різниці в якому форматі користувач здійснює підключення (в офісній мережі чи віддалене підключення за допомогою VPN).

Система надає декілька режимів роботи:

- Прозорий (Transparent) – забезпечує безшовний доступ до цільової системи без додаткової авторизації та використання веб-порталу. Користувач звертається до адреси кінцевого ресурсу та не бачить, що трафік проходить через Fudo PAM. Цей режим використовується лише тоді, коли необхідно провести непомітний для користувача моніторинг його дій рис.1.3.

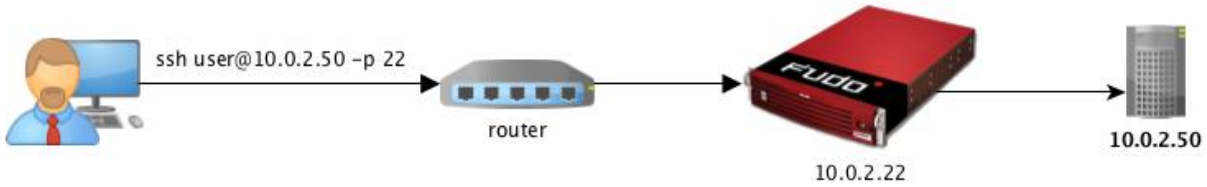

Рис.1.3. Схема мережі при режимі роботи Transparent

- Проксі (Proxy) – пропонує підключення до необхідних ресурсів через портал самообслуговування. Звернувшись до Fudo PAM і авторизувавшись там через веб-інтерфейс, користувач побачить список доступних йому серверів та програм рис.1.4.

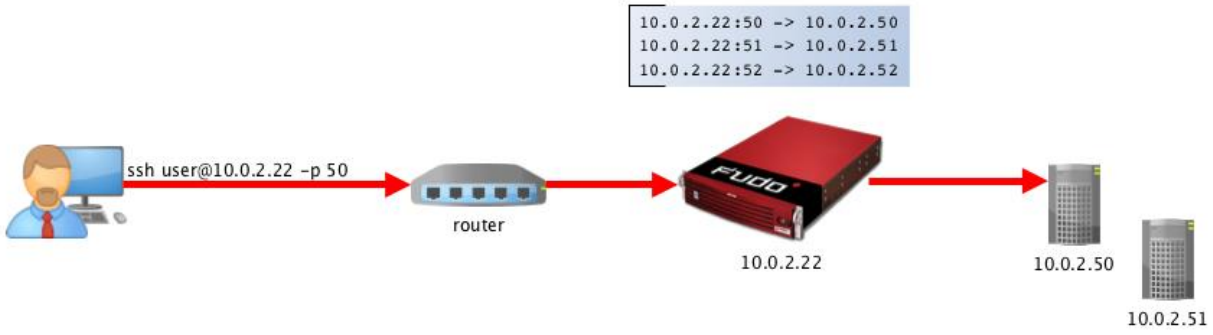

Рис.1.4. Схема мережі при режимі роботи Proxy

- Шлюз (Gateway) — у режимі шлюзу користувачі підключаються до цільового сервера за його фактичною IP-адресою, проте Fudo PAM забезпечує з'єднання з цим сервером, використовуючи власну IP-адресу. Такий підхід дозволяє приховати фактичну IP-адресацію та налаштовувати сервери так, щоб вони приймали лише запити Fudo PAM на рис.1.5.

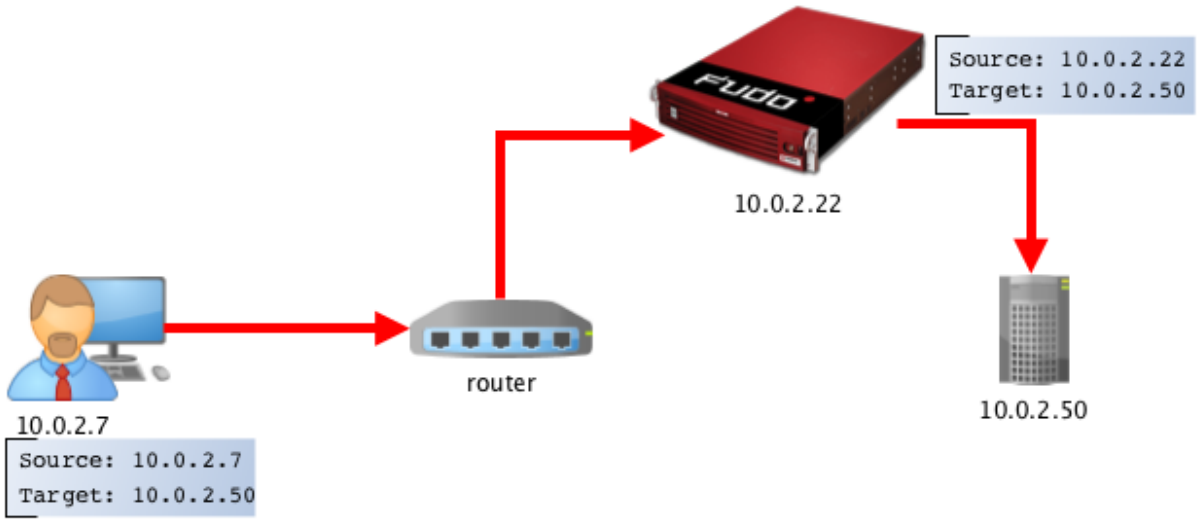

Рис.1.5 Схема мережі при режимі роботи Gateway

- Бастіон (Bastion) - при використанні цього режиму обліковий запис на цільовому хості або сам хост вказуються в рядку, що ідентифікує користувача, наприклад «ssh oskrypnik#admin@10.0.2.22». Це дозволяє спростити доступ до групи серверів, що відстежуються, за допомогою однієї і тієї ж комбінації IP-адреси і номера порту. Також цей режим роботи є захищеним і рекомендується для організації роботи зовнішніх підрядників (коли має сенс максимально приховати інформацію про внутрішню IT-інфраструктуру організації), рис.1.6.[5]

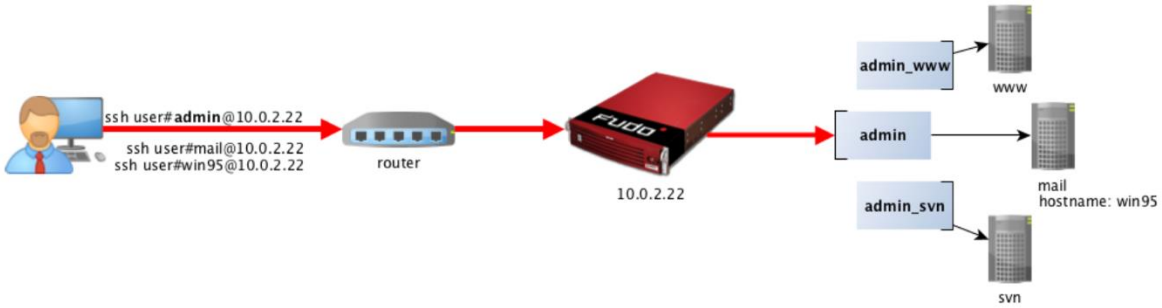

Рис.1.6. Схема мережі при режимі роботи Bastion

1.5. Огляд системи на Fidelis Network and Deception

Fidelis Network and Deception є професійним рішенням у підході до захисту інформаційної системи компанії. Тому що має достатні функціональні можливості для здійснення комплексного захисту тобто реагування на несанкціоновані дії та формування аналітичної звітності на основі отриманих статичних даних.

Fidelis Network and Deception має єдину консоль управління, яка об’єднує в собі можливість здійснювати управління всіма компонентами рішення.

Fidelis Network має такі компоненти, як консоль управління, колектор, сенсор (Direct, Internal, Web, Mail).

Fidelis Deception включає у собі компоненти, як консоль управління, сервіс пасток.

На даній схемі можна побачити схему взаємодії між компонентами системи рис 1.7.

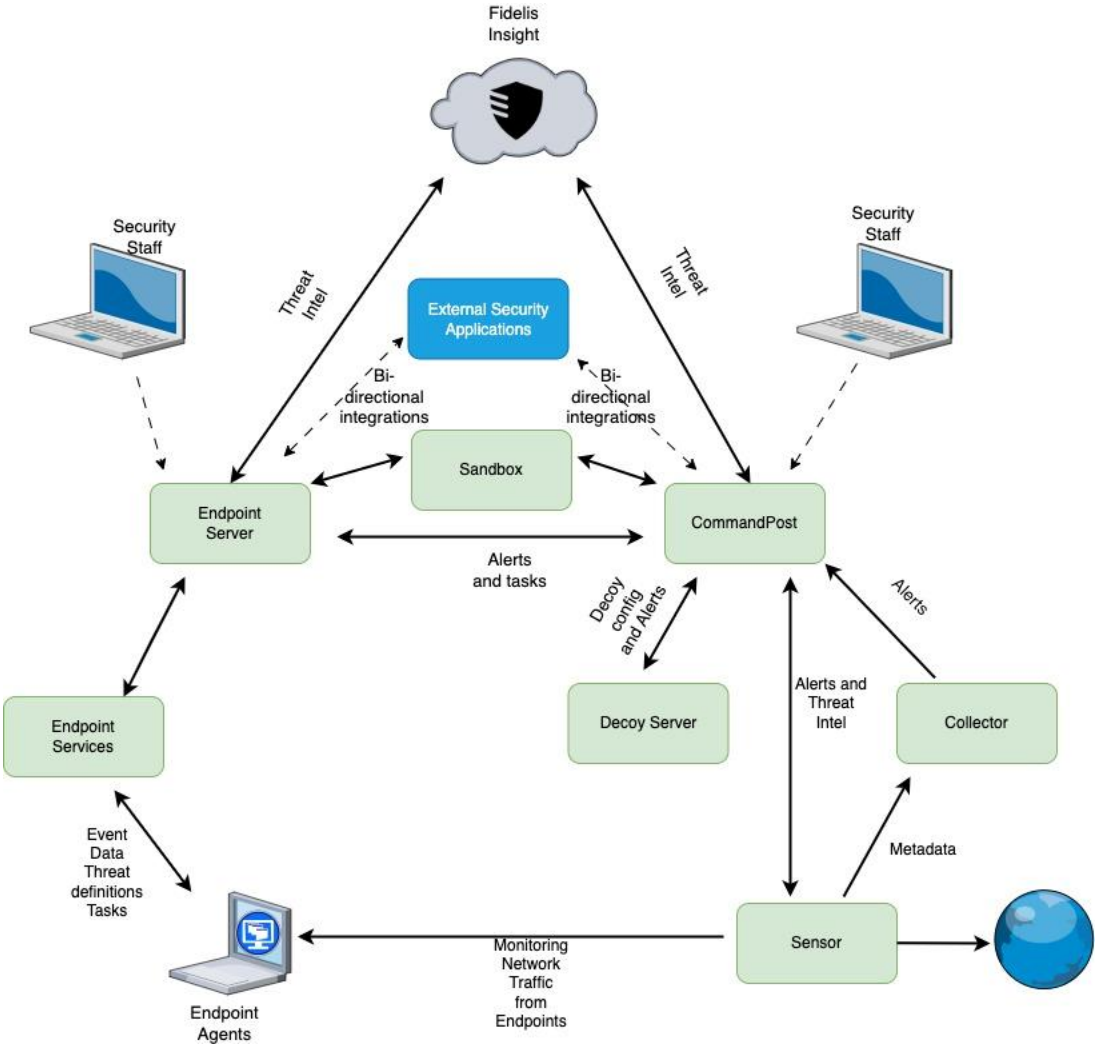

Рис.1.7. Схема взаємодії компонентів

Надалі розглянемо ключові компоненти, які допомагають здійснювати функціонування системи.

Основний компоненти, який присутній у кожному модулі це CommandPost, за допомогою, якого можна здійснювати управління всією системо та перегляд, реагування на інциденти.

У рішенні Fidelis реагування на інциденти відбувається за допомогою сенсорів, які реагують на вразливості.

Sensore Fidelis Direct бачить і керує двонаправленим трафіком у точках входу та виходу, відстежуючи та впроваджуючи політику для всього відомого та невідомого мережевого трафіку, протоколів і програм на швидкості з’єднання. Sensore Fidelis Direct, як правило розгортають на периметрі мережі, вбудовані або поза смугою для моніторингу додатків і

протоколів. Fidelis Direct працює в потоковому режимі, тому трафік не зупиняється для аналізу. Цей сенсор не дає майже нульову затримку в мережу, навіть якщо його розгортати в мережі. Fidelis Direct може забезпечити виконання правил запобігання як вбудованим, так і позасмуговим.

Аналізуючи відстежуваний трафік, сенсор Fidelis Direct може ідентифікувати та класифікувати активи, які передаються через сенсор. Класифікація включає визначення операційної системи та ролі активів, таких як робоча станція, поштовий сервер, DNS-сервер або пристрій IOT.

Fidelis Internal Sensore відстежує внутрішній мережевий трафік, забезпечуючи безпрецедентний рівень видимості та контролю того, як інформація використовується та зловживається на підприємстві. Внутрішні сенсори зазвичай розгортаються в ядрі мережі, щоб забезпечити видимість і контроль інформації, що виходить з центрів обробки даних або передається між підрозділами.

Fidelis Internal працює в потоковому режимі, тому трафік не зупиняється для аналізу. Сенсор додає майже нульову затримку в мережу, навіть якщо її розгортати в мережі. Цей сенсор може застосовувати правила запобігання, як вбудованому, так і поза смугою, однак запобігання не може бути гарантовано.

Аналізуючи відстежуваний трафік, внутрішній сенсор Fidelis може ідентифікувати та класифікувати активи, які передаються через сенсор. Класифікація включає визначення операційної системи та ролі активів, таких як робоча станція, поштовий сервер, DNS-сервер або пристрій IOT.

Fidelis Web sensore пропонує інтерфейс для стороннього пристрою за допомогою протоколу адаптації Інтернет-контенту (ICAP). ICAP — це легкий і розширюваний протокол «точка-точка», який використовується для запиту послуг для перевірки вмісту. ICAP доступний з багатьох пристроїв безпеки, включаючи веб-проксі, FTP-сервери, безпечні файлові сервери

електронної пошти та Cloud Access Security Brokers (CASB). Fidelis Web може виконувати перевірку вмісту для будь-якого з цих пристроїв.

Fidelis Mail sensore відстежує та впроваджує політику трафіку електронної пошти, надаючи параметри карантину, сповіщення відправника, видалення вкладених файлів і перенаправлення. Є можливість розгортати продукти з сенсором пошти в SMTP-шляху в режимі MTA, у позасмуговому режимі BCC або за допомогою шлюзу електронної пошти з підтримкою Milter.

Fidelis Mail sensore в режимі MTA працює в режимі зберігання та пересилання. У цьому режимі може бути гарантована профілактика та карантин для будь-якої електронної пошти, яка порушує політику. У режимі BCC сенсор працює з копією електронної пошти, яка не розміщена на шляху пересилання електронної пошти. У режимі milter сенсор пошти залежить від стороннього MTA для профілактики та карантину.

Fidelis Deception використовує ті самі сенсори, що й Fidelis Network. Якщо сенсор використовується і для Network, і для Deception, застосовуються операції, описані для Fidelis Network. Якщо сенсор використовується виключно для Fidelis Deception, до Deception буде застосовано лише параметр Asset Discovery.[5]

Сенсор аналізує весь трафік, щоб виявити і класифікувати всі активи, передані через нього. CommandPost буде зберігати базу даних активів, щоб перерахувати ці активи і надати інформацію, включаючи операційну систему і роль об'єкта, а також виявлені пристрої IoT. База даних об'єктів використовується для автоматизації створення та розповсюдження приманок на серверах приманок. Приманки також можна створювати вручну в CommandPost.

На сервері приманок розміщені всі приманки в мережі. Приманки - це фальшиві активи, визначені в мережі. Зловмисник може взаємодіяти з приманкою для входу в систему, доступу до файлів і зберігання файлів у системі. Усі дії записуються, а доступ до приманки, призводить до

сповіщення про неї. Приманки можуть бути на основі емуляції або RealOS. Приманки на основі RealOS використовують внутрішнє віртуальне середовище для запуску образів різних машин. Існують образи за замовчуванням, які можуть бути частиною початкового налаштування, або користувач може створити свій власний образ машини, як "золотий образ". Кількість приманок, які можна створити на кожному сервері приманок, залежить від типу сервера приманок.

1.6. Огляд системи на Symantec Web Security

Основний виток інформації та проникнення на внутрішній периметр організації відбувається через мережу Інтернет, тому забезпечити комплексний підхід щодо захисту веб-безпеки є ключовим завданням офіцера безпеки.

Програми вимагачі які представлені в мережі – категорія програм, які здійснюють шифрування документів та даних, які надалі є не придатні для використання, а також здійснюється блокування до інших функцій комп’ютера. Дані програми є ключовим заробітком зловмисників тому що йде примушення жертв сплатити викуп за надання доступу.

Symantec Web Security є комплексним підходом щодо протидії зловмисникам отримати інформацію через мережу Інтернет. Дане рішення має в собі такі інструменти, які виконують захисні функції для забезпечення інформаційної безпеки.

ProxySG – використовується, як проксі сервер, за допомогою, якого здійснюється проксування дій, запитів користувачів в мережі. За допомогою даного компоненту можна здійснити автоматизоване спрацювання на правила прописані в системі. Є внутрішня БД ресурсів, які оцінюється вбудованою системою ризиків, згідно яких виконується аналіз дій користувачів.

Symantec Content Analysis — це антивірусна система нового покоління, виявлення шкідливих і шпигунських програм. Content Analysis містить такі функції:

- Сканування зловмисного програмного забезпечення та антивірусне сканування — Content Analysis підтримує антивірусні механізми та бази даних вірусних сигнатур Symantec, Kaspersky, McAfee та Sophos. Ви можете використовувати один або два AV-процесори з аналізом вмісту.
- Прогнозний аналіз — Додаткові послуги передплати від Symantec і Cylance використовують вдосконалений механізм штучного інтелекту для виявлення зловмисного програмного забезпечення.
- Служба репутації файлів — Content Analysis генерує хеші SHA1, MD5 і SHA-256 для кожного файлу, який вона обробляє. Ці хеші порівнюються з хмарною службою класифікації репутації файлів Symantec для ідентифікації відомих файлів. Служба використовує показники репутації, числа (1–10), які вказують на те, чи є файли надійними чи шкідливими; низькі бали менш імовірно будуть загрозою, тоді як високі бали більш імовірні. Залежно від оцінки репутації файли блокуються, якщо оцінка висока, або передаються користувачеві як безпечні, якщо оцінка низька, або обробка продовжується з антивірусним скануванням і ізольованим програмним середовищем, якщо служба не знає, чи файл є зловмисний.[7]
- Чорний і білий список файлів, створений вручну. Оскільки ваша організація визначає файли, які відомі як хороші чи погані, ви можете додати їх до списку визначених вручну хешів файлів, щоб дозволити або заборонити ці файли без подальшої обробки.
- Інтеграція пісочниці із зовнішніми постачальниками (Symantec Malware Analysis, Lastline або FireEye) — служби пісочниці

використовують різні методи для визначення дій, які виконує виконуваний файл на робочій станції клієнта, зокрема веб-запити зловмисних URL-адрес і зміни системних файлів.[8]

- On-box Sandboxing — Пропонує зручність аналізу підозрілих файлів за допомогою Content Analysis без необхідності купувати та інтегрувати зовнішній пристрій ізольованого програмного середовища.
- Інтеграція кінцевої точки — коли пісочниця виявляє зловмисне програмне забезпечення, Content Analysis може запитувати сервер CounterTack Sentinel у вашій мережі, щоб визначити, які користувачі (якщо такі є) отримали його. Якщо Symantec Endpoint Protection Manager (SEPM) інтегровано з Content Analysis, адміністратор отримує сповіщення, коли пісочниця знаходить шкідливий файл, і надає можливість додати хеш файлу до чорного списку в SEPM.
- Кешовані відповіді — коли модуль аналізу вмісту визначає вердикт (чистий чи зловмисний) для файлу, він кешує хеші файлів і вердикти, щоб уникнути необхідності сканувати той самий файл під час наступних запитів. Content Analysis має окремі кеші для відповідей від кожної зі своїх служб: антивірус, репутація файлів, прогнозний аналіз і пісочниця (загрози та чиста).
- Symantec Global Intelligence Network (GIN) — користувачі захищені базами даних Symantec WebFilter і GIN на пристрої ProxySG, і коли під час сканування виявляється зловмисне програмне забезпечення, ці результати можна надіслати WebFilter для класифікації шкідливих URL-адрес на користь усіх користувачів GIN у всьому світі.

Management Center – компонент для централізованого управління та контролю пристроями Symantec у організації.

Можна організовувати пристрої в ієрархічні групи, контролювати стан пристроїв, установлювати політики на пристрої ProxySG, створювати резервні копії конфігурацій пристроїв і створювати консолідовані звіти.

Крім того, є можливість контролювати доступ до Центру управління та пристроїв. Також можна контролювати доступ, додаючи користувачів системи вручну або пройшовши автентифікацію за допомогою існуючого каталогу чи служби, наприклад RADIUS.

Reporter створює інтуїтивно зрозумілі звіти для спеціалістів із безпеки, керівників відділів, менеджерів з персоналу та мережевих адміністраторів, яким потрібна видимість усієї активності користувачів у Інтернеті.

Symantec Reporter забезпечує масштабований збір журналів і зберігання як пристрій або віртуальний пристрій для кількох продуктів Symantec:

- ProxySG
- Розширений безпечний шлюз
- Служба веб-безпеки
- Аналіз вмісту
- Зворотний проксі
- Розгортання ProxySG у брандмауері веб-додатків

Symantec Reporter є ключовим компонентом рішення Secure Web Gateway. Reporter створює та відображає звіти на основі даних журналу доступу до веб-трафіку. Аналіз звітів дає уявлення про цілісність мережі та звички користувачів у веб-перегляді та відповідність політикам.

1.7. Постановка задачі

В наш час, інформаційні технології активно розвиваються та дають можливості автоматизувати методи захисту компанії, що мінімізує ризики, цільової атаки, яка буде націлена на конкретну систему в компанії.

Тому метою кваліфікаційної роботи є підвищення рівня інформаційної безпеки організації за рахунок системи моніторингу та боротьби з кіберзагрозами із застосуванням керування привілейованим доступом (PAM) Fudo, виявлення вразливостей цілеспрямованих атак (EDR) Fidelis, системи безпеки веб додатків (WSS) Symantec

Для досягнення поставленої мети необхідно вирішити такі завдання:

- провести аналітичний огляд предметної області роботи IT компанії «Oberig-IT» та узгодити всі ключові аспекти роботи компанії, визначити основні напрямки для розробки системи;
- провести аналіз існуючих кінцевих робочих станцій та визначити мережеву архітектуру;
- визначити технології та засоби для розробки системи;
- провести аналіз впроваджених рішень для подальшої сумісності та інтеграції з розробленою системою;
- проаналізувати правила доступності систем;
- визначити вразливі місця в системі інформаційної безпеки компанії «Oberig-IT» (робота підрядних компаній в інфраструктурі, стеження за електронною поштою, яка надходить від невідомих користувачів «фішинг»);
- розробити оптимізовані рішення за допомогою кастомізації та написання скриптів;
- спроектувати базу даних MS SQL;
- розробити систему моніторингу та боротьби з кіберзагрозами на базі WSS, EDR та PAM рішень.

Перевагою розробленої системи захисту є можливість здійснювати прозорий моніторинг системи, що допоможе в подальшому швидко, або навіть в автоматизованому режимі приймати рішення щодо захисту системи. В цілому розроблений комплекс допоможе підвищити інформаційну безпеку організації та зберегти IT-інфраструктуру компанії неушкодженою.

1.8. Висновки до розділу 1

На сьогодні більшість компаній збільшують фінансування в напрям кібер-безпеки компанії, що є критичною необхідністю для ефективного функціонування бізнесу. Існує безліч методів атак, які можуть бути спрямовані на інформаційні системи компанії. Найпопулярнішою атакою є DDos, яка спрямована на виведення з експлуатації устаткування або електронні ресурси, шляхом надсилання великого об’єму трафіку. Другий за популярністтю методів атака є фішинг, за допомогою даної тактики, зловмисник може підробити легітимний веб-ресурс.

Згідно тенденцій системи кіберзахисту, корисним для розрахування вартості виконаних робіт підрядниками, як системи PAM, які здійснюють повний контроль записом дій користувача форматі відео та логування. Додатково дані системи можуть не лише мінімізували ризик злочинних дій, а й зменшити документообіг в середині організації шляхом відправки запитів адміністраторам системи на доступу, до тих чи інших систем.

РОЗДІЛ 2

ТЕХНОЛОГІЇ ТА ІНСТРУМЕНТИ ДЛЯ СТВОРЕННЯ СИСТЕМ АНАЛІЗУ ТА БОРОТЬБИ З КІБЕРЗАГРОЗАМИ

На сьогоднішній день системи, які призначені для аналізу та протидії кіберзагрозам, виконують безліч задач. Основна з них – це мінімізація ризиків та автоматизована протидія ним. Рішення потрібно розглядати концептуально, враховуючи які використовуються в роботі та дивитися на тенденцію потреб на ринку. Можна провести аналітичний розбір вимог замовників. Першою головною проблемою всіх великих організацій це є співробітник та підрядники, які виконують певні дії в цільових системах компанії.

Тобто постає питання, як можна здійснювати контроль за користувачами або привілейованими користувача? Саме привілейовані користувачі мають доступ до конкретних цільових систем організації, це може бути, як веб-ресурс так і якийсь сервер. В ході роботи маємо мету відшукати певні рішення, які будуть закривати певні проблеми та побудує певний захисний шар внутрішнього периметру організації.

Побудова таких рішень потребує реалізацію певних допоміжних компонентів, які будуть виконувати механіку роботи рішення. До прикладу це розробка спеціального агенту, за допомогою, якого буде відбуватися моніторинг дій користувача та демонструвати повний ландшафт екосистеми користувача з відображенням встановленого програного забезпечення. Або

здійснювати детекцію дій користувача підчас встановленого з’єднання до цільової системи з повним аналізом дій сесії та записом.

2.1. Технології для розробки систем захисту

Для впровадження рішень, WSS, PAM, EDR, насамперед потрібно мати можливість здійснювати вичитку користувачів з Active Directory, даний функціонал необхідний для полегшення авторизації користувачів та додатково для розгортання політик та агентів відповідно до рішення.

В основі Fidelis (EDR) та Fudo (PAM), лежать розгорнуті бази даних. Відповідно до рішення це Microsoft SQL та PostgreSQL. Дані бази даних виконують такі функції, як збереження конфігураційних даних системи. Лише якщо дивитися в розріз Fudo PAM це є інтегрована БД PostgreSQL, яка розгортається відразу з appliance, який побудований на операційній системі FreeBSD. Рішення Fidelis (EDR) потребує додаткового розгортання Microsoft SQL.

Якщо є потреба здійснити звернення до БД то, як правило використовується запити на основі SQL.

SQL – це мова, яка використовується серед спеціалістів, для забезпечення доступу та керування вмістом бази даних. Основним плюсом, можна виділити так це швидкодію виконання запита користувача та її простота у здійснені запиту.[9]

Якщо розглядати принцип процесу взаємодії, то MySQL побудована на основі клієнт-сервера, згідно чого можна зробити висновки, що клієнт даній зв’язці буде відігравати користувацький інтерфейс за допомогою, якого користувач, буде здійснювати відповідні запити, а сервер це певний обчислювальний пристрій, який має достатню кількістю виділених ресурсів для опрацювання запитів користувача, тобто команди.

На такій же самій основі і побудована реалізація PostgreSQL, де також є сервер, який буде опрацьовувати запити користувача та надавати відповідні

відповіді на них. Додатково в даних рішеннях можна побудувати навіть відмовостійку систему БД, яка в разі чого зможе відіграти будь-які спрямовані на неї атаки, наприклад DoS атаку.

За основу дані рішення побудовані на основі операційних системах сімейства Linux. Тож управління адміністративними можливостями системи відбувається за допомогою команд в CLI консолі в appliance. В реалізації даної дипломної роботи було опрацьовано такі операційні системи, як Windows, FreeBSD, Centos7.

2.2. Побудова функціональної складної системи Fudo PAM

Необхідно розробити програмне рішення, яке націлене на адміністрування привілейованих користувачів Fudo PAM. Існує вбудоване «програмне середовище», за допомогою, якого можна здійснювати інтеграційні дії та розробляти додаткові програмні засоби, які в свою чергу розширюють функціонал системи.

Fudo PAM має в основі операційну систем Unix, Free BSD, тому для початку роботи потрібно розгорнути систему в обраному середовищі віртуалізації. Fudo PAM постачається у вигляді ova / ovf образу, та підтримує такі середовища розгортання, як Hyper-V, VirtualBox, KVM, VMware. [10] В даній роботі, буде використана система віртуалізації VMware. Після того, як буде розгорнуто рішення потрібно пройти кілька кроків, для отримання веб-консолі, управління. Основні кроки, це надання паролю, який буде використовуватися для шифрування БД, та надання IP-адрес для отримання доступу на веб-ресурс. Якщо всі кроки, були виконані то маємо отримати доступ до консолі управління, рішення, звідки можна здійснювати управління системою рис.2.1.

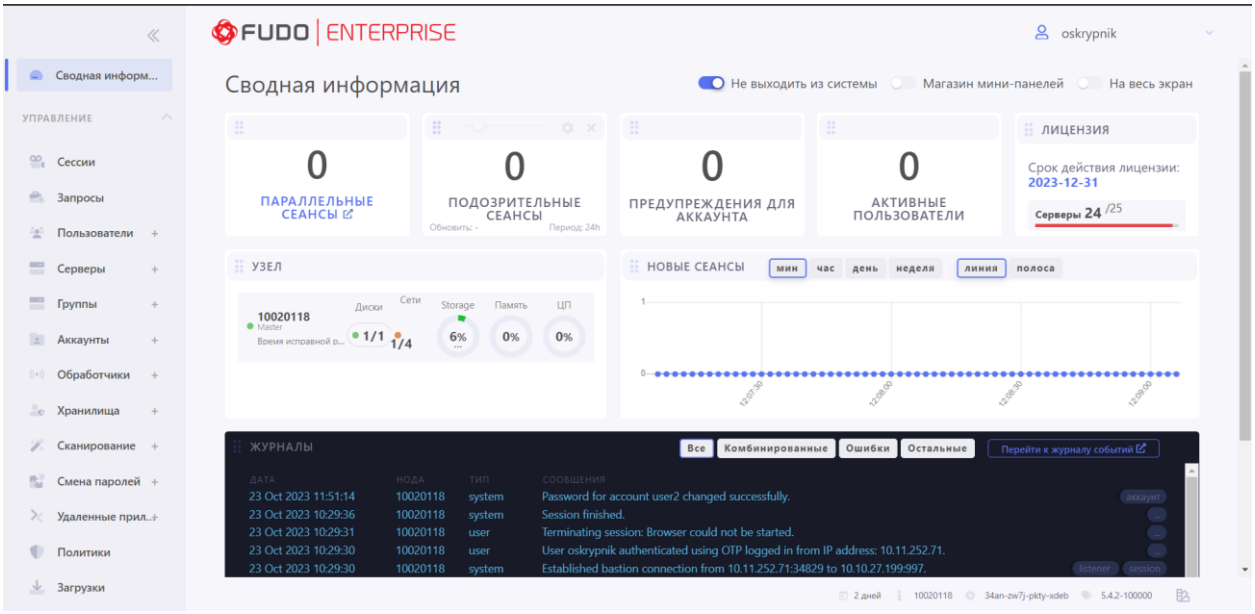

Рис.2.1. Адміністративна консоль управління

2.3. Підготовка до роботи функціональної складної системи Symantec WSS

Для того щоб система функціонувала в повному обсязі потрібно розгортати всі модулі, які до нього входять, а саме це ProxySG, Management Center (MC), Reporter, Content Analysis System (CAS).

Усі ці модулі побудовані на операційній системі сімейства Linux, Centos7. Для початку потрібно розгорнути віртуальний аплаінс, для того щоб розпочати повну взаємодію з системою та її доповненням функціональних можливостей. Всі рішення даного виду мають в собі proxy, який виконує роль проксування користувацького трафіку через себе, але вже з розробленими політиками, які накладаються та проводиться аналіз трафіку.

Всі компоненти постачаються окремо вигляді ova образу, та підтримує такі середовища розгортання, як Hyper-V, VirtualBox, KVM, VMware. Для початку робіт, є необхідність лише надати IP-адреси віртуальним аплаінсам та почати конфігурацію да кастомізацію через вбудоване середовище в веб-інтерфейсі.

В Symantec WSS центральною веб-консоллю управління виступає Management Center (MC), з даним модулем потрібно провести синхронізацію з іншими компонентами системи. Згідно аналізу та практики може використовуватися не по одному компоненту системи (наприклад, можна використовуватися дві чи три ProxySG, для відмовостійкості чи розміщення модуля ProxySG в різних ЦОД).

Тому коли вже всі модулі розгорнуті та додані в систему можемо бачити наступне рис.2.2-2.3.

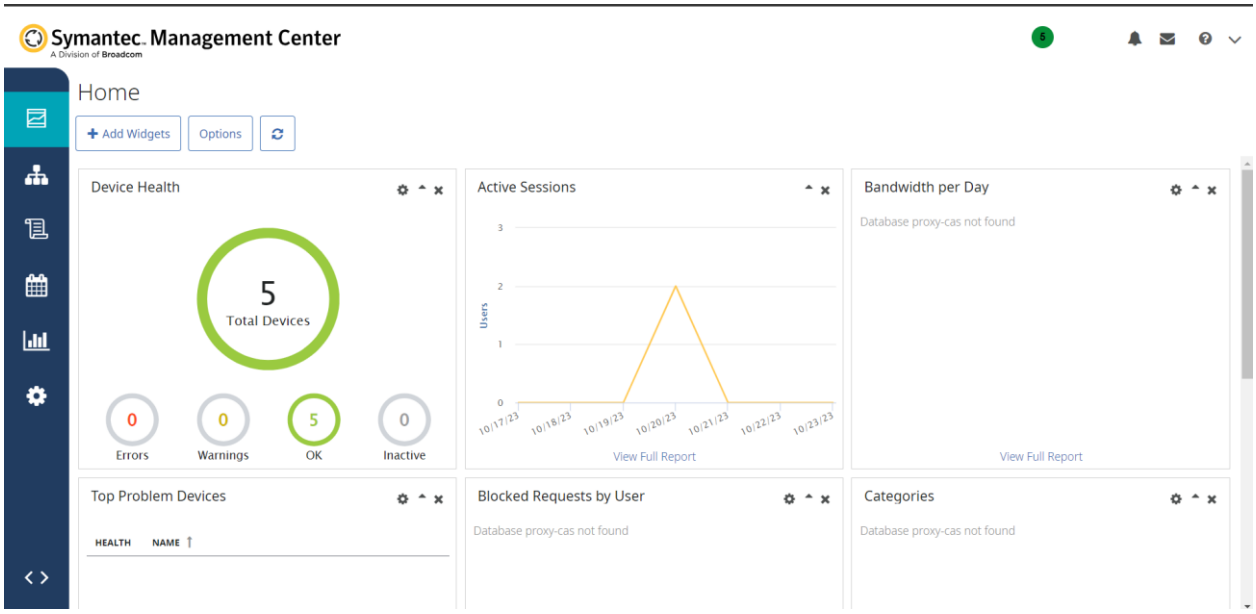

Рис.2.2. Центральна консоль управління (Management Center)

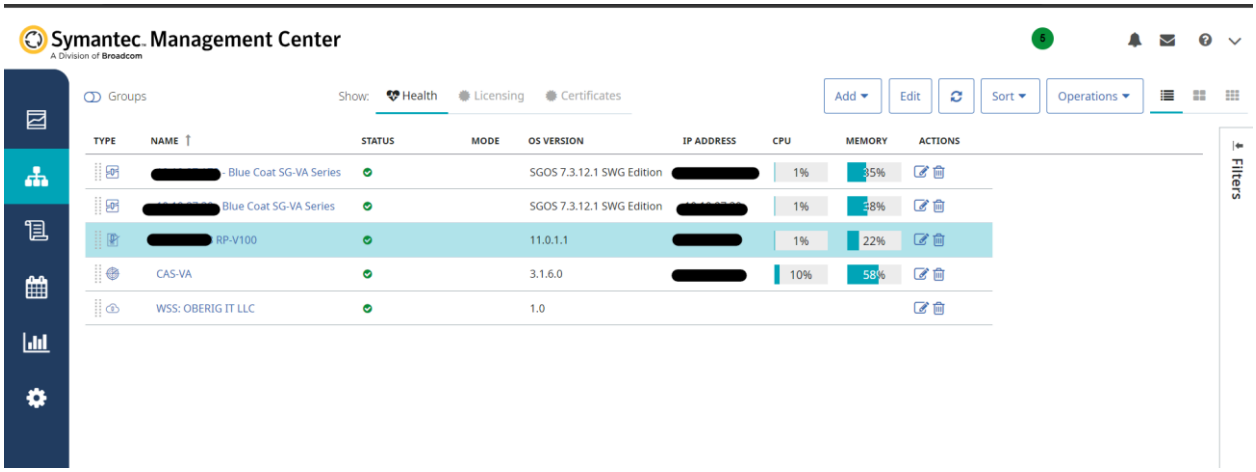

Рис.2.3. Інтегровані компоненти в центральній консолі управління (Management Center)

2.4 Впровадження функціональної складної системи Fidelis Elevate

Fidelis Elevate, має будову багато модульного рішення, та ділиться на модулі та компоненти, тому для повноцінного розгортання потребує досить ресурсну систему.

В свою чергу коли дана система повноцінно інтегрована в IT-середовище компанії, дає повну інформацію про мережевий трафік в середині організації, та реагує на кіберінциденти в автоматизованому режимі за допомогою написаних правил та застосування політик.

В основі рішення лежить операційна система Centos7. Тому є необхідність в розгортанні Network та Deception мають спільну консоль управління рис.2.4.

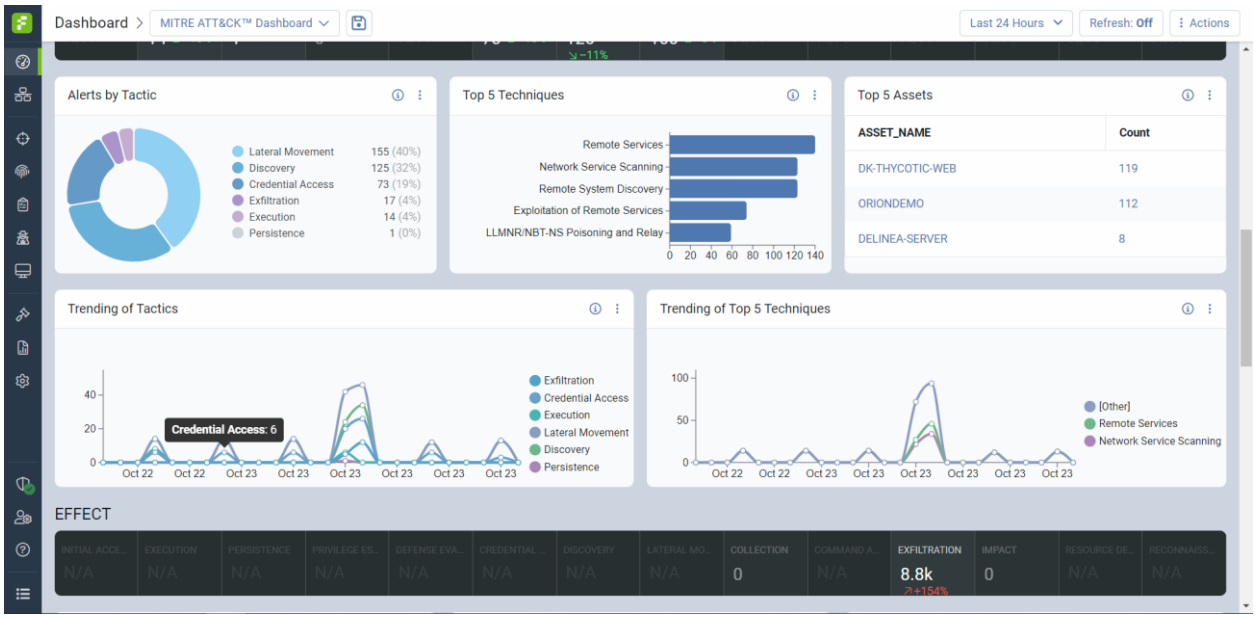

Рис.2.4. Консоль управління Network та Deception.

В подальшому буде продемонстровано можливості кастомізації налаштувань, які будуть продемонстровані в реагуванні на інциденти.

EndPoint частина має окрему консоль управління, яка відповідає за кінцеву пристрої, це може бути, будь що, від серверів до звичайних комп’ютерів користувачів рис.2.5.

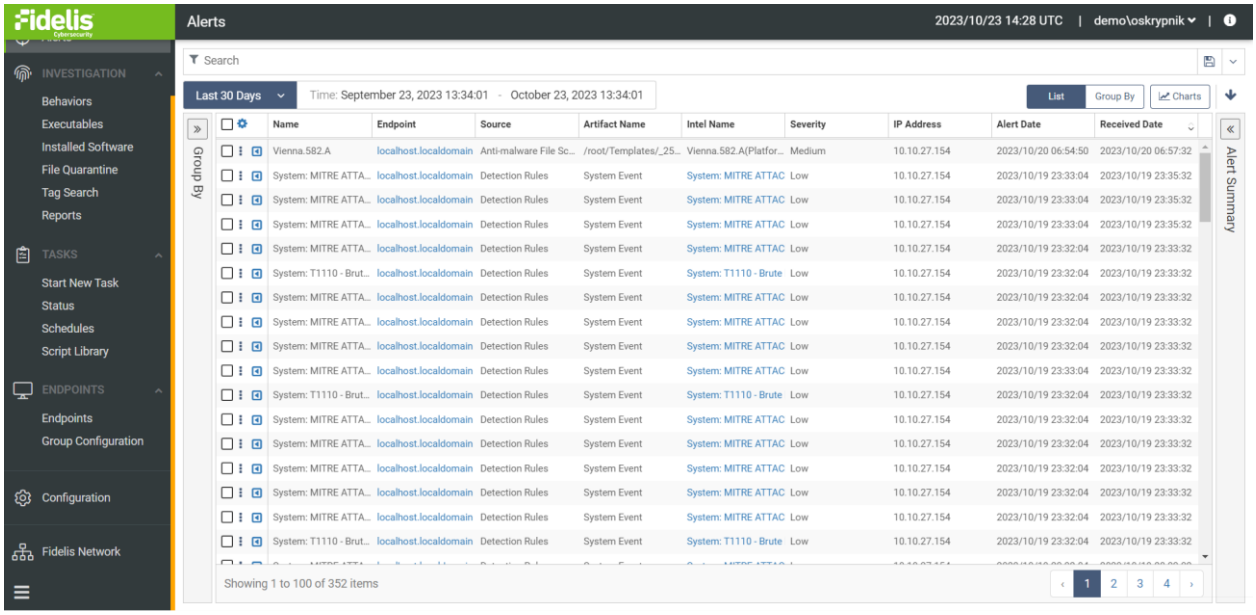

Рис.2.5. Консоль управління EndPoint модуля

На робочу станцію встановлюється агент, який виконує «опитування» системи на кшталт виявлення нових пристрої в мережі та побудова мапи, яка відображає топологію мережі. Звичайно даний модуль з‘єднаний з центральною консоллю управління, куди відбувається передача аналітичних даних для подальшого реагування, збирається аналітика кібербезпеки та цілої SOCK команди.

2.5. Розробка правил реагування на інциденти

В рішеннях, які відносяться до класу WSS, EDR, XDR, реагування на кіберінциденти відбувається за допомогою розробки «Yara» правил, які в свою чергу зацикленні на спрацювання на ключові дії з боку мережевого трафіку. Під час впровадження з «коробки», можна отримати базовий набір правил, але на даний момент їх стає не достатньо.

YARA — це багатоплатформна програма, що працює на Windows, Linux і Mac OS X. Правила YARA — це шаблони виявлення зловмисного програмного забезпечення, які можна повністю налаштувати для виявлення

цілеспрямованих атак і загроз безпеці, характерних для середовища, в якому відбувається впровадження рішення. Побудова YARA правила відбувається під час аналізу вразливого програмного забезпечення аналітиком інформаційної безпеки, коли відбувається виявлення, якихось унікальних шаблонів та структур вразливого програмного забезпечення. При аналізуванні одного сімейства вразливого програмного забезпечення можна написати одне YARA правило, спеціально для даного вразливого ПО.

Наприклад, в деяких системах YARA правила відображаються наступним чином fidelis рис.2.6.

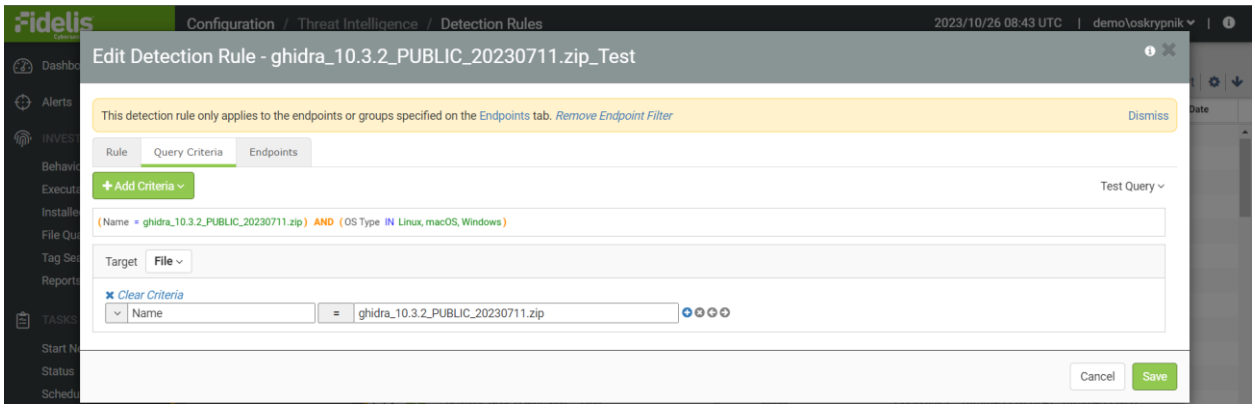

Рис.2.6. YARA правила в реалізації fidelis.

2.6. Розробка регулярних висловів для спрацювання правил

В деяких рішеннях реагування на дії користувачів, відбувається шляхом написання регулярних виразів, які містять логіку спрацювання в системі та сповіщення адміністратора.

Під час впровадження рішення в основному, як показує практика та аналіз рішень, регулярні вирази відсутні, тобто адміністраторам або інтеграторам потрібно писати регулярні вирази вручну.

Регулярні вирази – це є деяка послідовність символів, яка буде виявляти шаблон відповідності в тексті. Тобто відбувається пошук за конкретними виразами, які вказані в регулярному виразі.

В ході даної роботи логіка спрацювання на дії користувача в одному рішенні побудована на роботі регулярних виразів.

Fudo може реагувати на дії користувача за допомогою цих самих регулярних виразів. Тобто коли користувач ініціює з'єднання з кінцевою цільовою системою, наприклад по протоколу SSH, можемо створити для окремої групи користувачів спеціальний перелік команд, на які система буде реагувати різними діями, від надсилання сповіщення електронною поштою адміністратору, до повного розірвання з'єднання.

Наприклад, необхідно заблокувати команду, rm, яка може видалити певний файл з системи, тоді регулярний вираз матиме наступний вигляд:

(^|[^a-zA Z])rm[[:space:]]+([^[:space:]]+[[:space:]]*)?/full/path/to/a/file([[:space:]]|\;|$)

(^|[^a-zA-Z])rm[[:space:]]+.*justafilename

(^|[^a-zA Z]) – дана форма запису буде вказувати на те що має зчитуватися натискання клавіш тобто набраний текст.

Rm – спрацювання на відповідну команду.

[[:space:]] – спрацювання на натискання користувачем клавіши.

Далі прописується шлях до файлу та його назва. Дані регулярні вирази оптимізують роботу адміністраторів та мінімізують ризики, що користувач зможе завдати шкоди системі, та зменшує відсоток застосування соціальної інженерії, коли певного співробітника було скомпрометовано та змушено до вчинення неправомірних дій на систему.

Більшість систем такого типу додатково пишуть файли логування, за допомогою, яких в подальшому можна проводити аудит та розслідування, що до дій з боку користувачів.

2.7. Середовище розробки

Для розробки та оптимізації даних рішень, може бути будь-яке середовище, яке має зручність роботи для технічного спеціаліста.

В ході даної роботи використовувалися такі середовища, як Notepad++, PyCharm.

Notepad++ - це безкоштовний редактор коду, який підходить для написання скриптів саме для веб рішень тобто на мовою HTML та CSS. Даний редактор не навантажує систему та є невеликим за обсягом, що сприяє роботі системи [15].

PyCharm – це редактор коду, який був розроблений компанією JetBrains, що спеціалізується на розробці інструментів для програмування різними мовами, таких як Java, Kotlin, C#, F#, C++, Ruby, Python, PHP, JavaScript та багато інших. Заснована раніше під ім'ям IntelliJ, вона сьогодні надає різноманітні засоби для командної роботи та підтримки розробки провідних мов програмування.

2.8. Висновки до розділу 2

Реагування на кіберінциденти, сьогодні є пріоритетною задачею, будь-якого підприємства, особливо того де опрацьовуються персональні данні клієнтів: медичні та фінансові, державні установи. Методи стають все складнішими для стандартного виявлення, тому потребують автоматизації процесів на виявлення та реагування.

Після того коли замовник обрав рішення або напрям, відбувається впровадження, тобто розгортання даного рішення на площадці у замовника.

Згідно до того, яке рішення та що саме воно потрібує це може бути, як розгортання стандартного .ova образу, так і розгортання цілого сервера Microsoft Server. Додатково вимагається інсталяція бази даних Microsoft SQL.

При реалізації консолі управління всіх рішень, а це EDR, XDR, PAM, WSS, доцільно користуватися стандартної консоллю управління, яка постачається розробником та має вже готовий вбудований базовий функціонал з метою його розширення.

Якщо постає задача в кастомізації чи оптимізації деяких дій можливо буде потребуватися написання скрипта для реалізації цього, Python, який у свою чергу допоможе спростити роботу з даними системами.

РОЗДІЛ 3

РОЗРОБКА ТА АДМІНІСТРУВАННЯ СИСТЕМ EDR, PAM, WSS

При дослідженні та написанні даного кваліфікаційної роботи, було проаналізовано найкращі рішення, які задовольняли потреби замовника та були впровадженні в ІТ-систему організації «ОБЕРІГ-ІТ». Компанія ОБЕРІГ-ІТ є основним дистриб'ютором ІТ-рішень, які широко використовуються в проектах, також відповідають світовим тенденціям сьогодення. Сьогодні є основною платформою для розвитку бізнесу у сфері кібер-безпеки та інноваційних ІТ-технологій для партнерів-інтеграторів, вендорів та кінцевих замовників. Організація має широку мережу представництв по світу та нараховує близько 250 співробітників та близько 60 партнерів, з якими виконуються проекти.

Підчас проведення, аудиту інформаційної безпеки в організації ОБЕРІГ-ІТ, було виявлено ряд проблем та побажань зі сторони співробітників компанії. Першою та основною проблемою була робота підрядних фірм в інформаційному середовищі компанії. Для роботи підрядників потрібно створювати облікові записи та надавати авторизаційні данні. На додаток до цього є необхідність в контролі дій підрядника під час виконання регламентних робіт. Другою проблемою, яку було виявлено це необхідність обмежувати та контролювати доступ користувачів до веб-ресурсів, з відповідним аналізом трафіку. Третя проблема, яка була знайдена, полягає в здійсненні захисту цільових систем шляхом розкидання пасток для введення в оману зловмисника.

3.1. Розгортання комплексів PAM, WSS, EDR

Для початку роботи, потрібно проаналізувати данні в ході, після чого буде визначено для PAM рішення, визначено кількість цільових систем, кількість одночасних підключень до них. Це необхідно щоб надати відповідні ресурси для розгортання аплаінсів на віртуальному середовищу HyperView. При інтеграції ряд рішень в роботі мають на меті розгортання БД та виділення відповідних ресурсів для стабільної роботи. Оскільки в Fudo PAM БД є вбудована та при розгортанні буде зашифрована, та зберігатиме в собі інформацію про користувачів та записані сесії, потрібно наперед прорахувати її вміст. Так як в нас 250 користувачів та цільових систем буде 25 в основному це підключення по протоколу (ssh, rdp, http/https), та одночасних сесій планується до 4 на один цільовий хост.

Етапи розгортання Fudo PAM представленні на рис. 3.1 – 3.3.

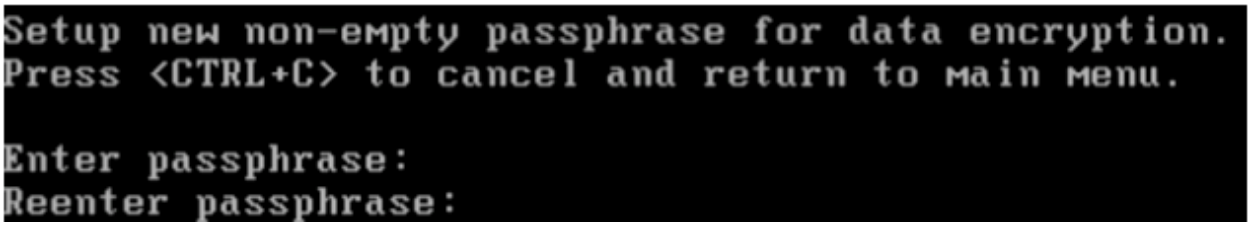

Рис. 3.1. Етап шифрування БД PostgreSQL.

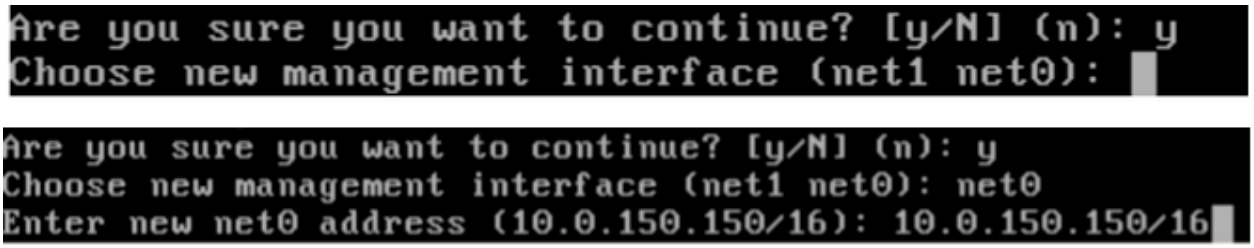

Рис. 3.2. Обрання інтерфейсу.

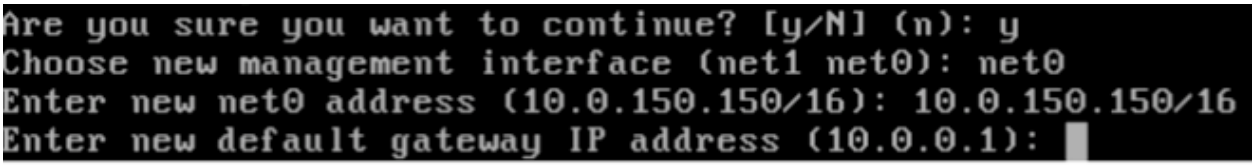

Рис. 3.3. Надання мережевих налаштувань.

При проектуванні програмного комплексу Fidelis EDR, потрібно розуміти, що дане рішення є багато модульним та вибагливим до виділених ресурсів тому, в даному випадку будуть використовуватися, вимоги які надасть вендор. Даний програмний комплекс включає в собі рішення для кінцевих робочих станцій та називається «Endpoint». Модулем, який потребує розгортання Windows Server 2016-2019, в нашому випадку буде розгорнуто на Windows Server 2016 та встановлено БД Microsoft SQL.

Етапи розгортання Fidelis EDR на рис.3.4-3.5.

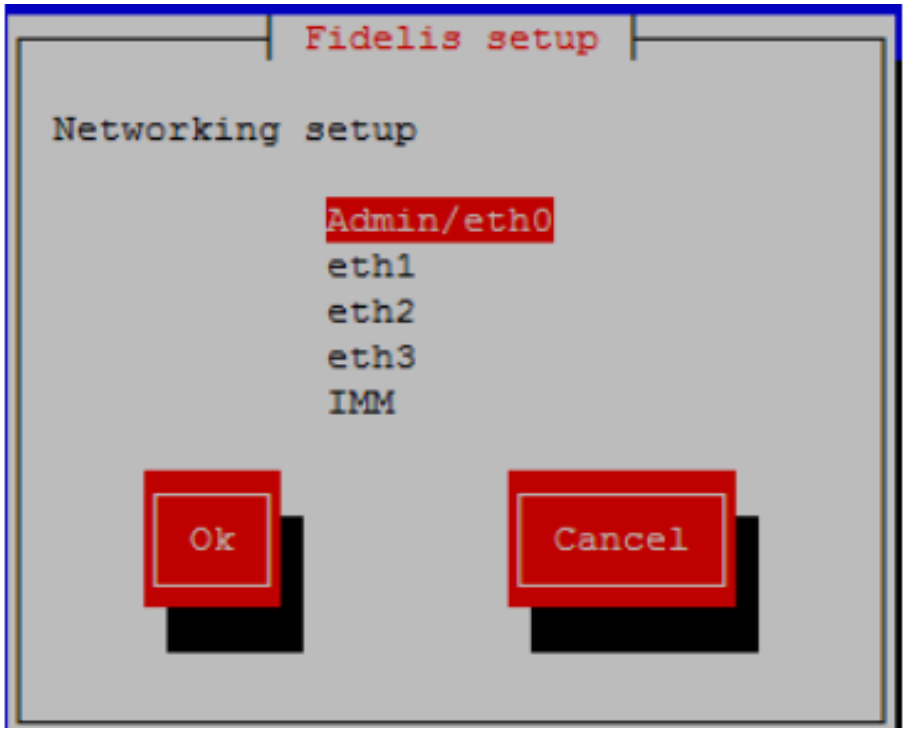

Рис.3.4. Обираємо мережевий інтерфейс.

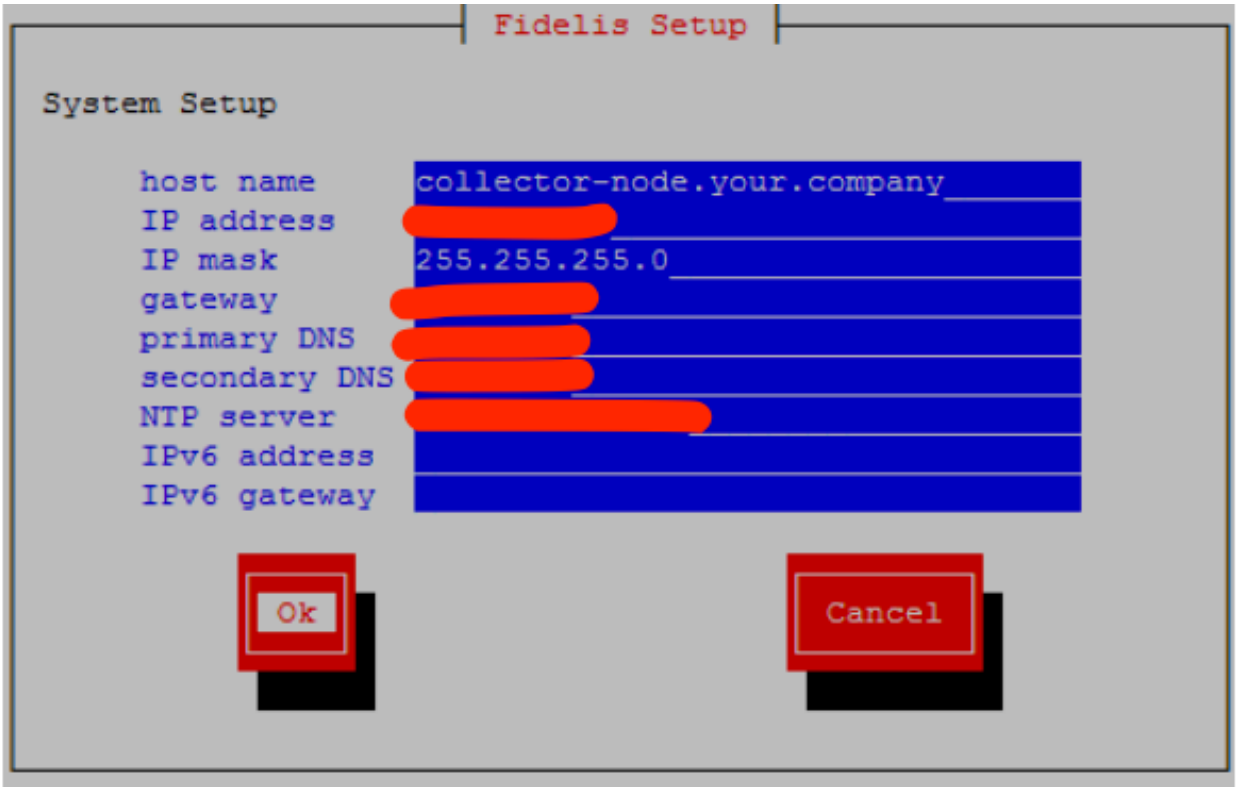

Рис.3.5. Заповнюємо мережеві параметри.

Symantec Web Security System є програмним комплексом, який включає в собі такі модулі, як ProxySG, CAS, Reporter, MC. Вони необхідні для повноцінної роботи системи. На вимогу замовника або згідно до поставлених вимог розгортання додаткових модулів, якщо є необхідність побудувати відмовостійкість системи, в даній компанії наявно два центри обробки даних (ЦОД), в яких будуть окремо розгортатися модулі системи.

Етапи розгортання Symantec Web Security System рис.3.6.-3.8.

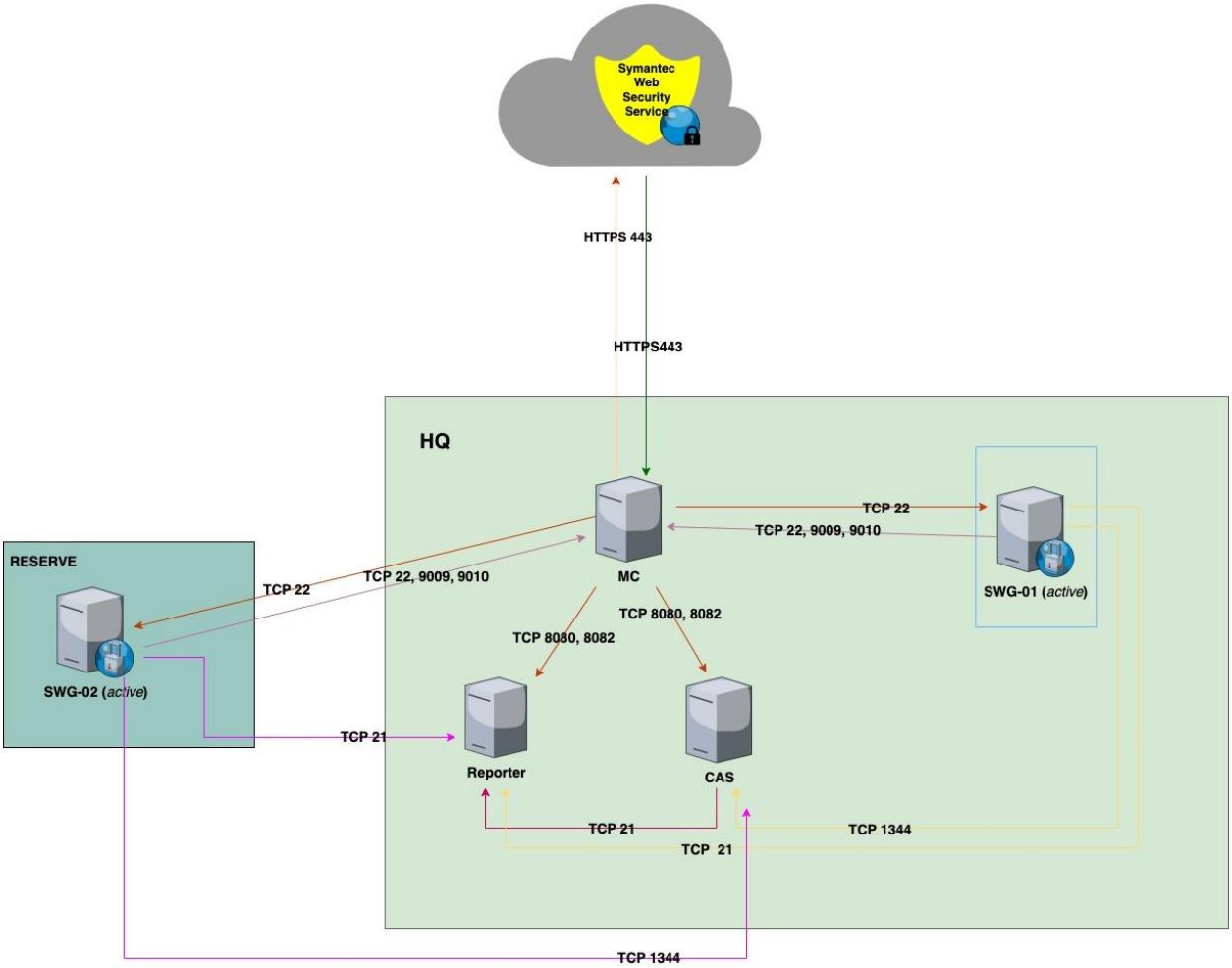

Рис.3.6. Архітектура побудови рішення

Із зображення на рис.3.1.7 можна зробити висновок, що буде реалізовано відмово стійкість за рахунок розгортання двох ProxySG серверів в різних ЦОД. Це дасть змогу в результаті виходу одного з робочого стану передати можливість пропускання трафіку та роботи системи іншому. Побудова даного кластеру буде в форматі Active-Active, що також буде розподіляти навантаження між двома серверами, що забезпечить роботу при атаці наприклад DoS. Якщо навіть трапиться ситуація з повним виходом із ладу двох серверів є хмарне рішення яке працює в форматі агенту на робочій станції та зможе пропускати через себе клієнтський трафік та накладати на нього політики.

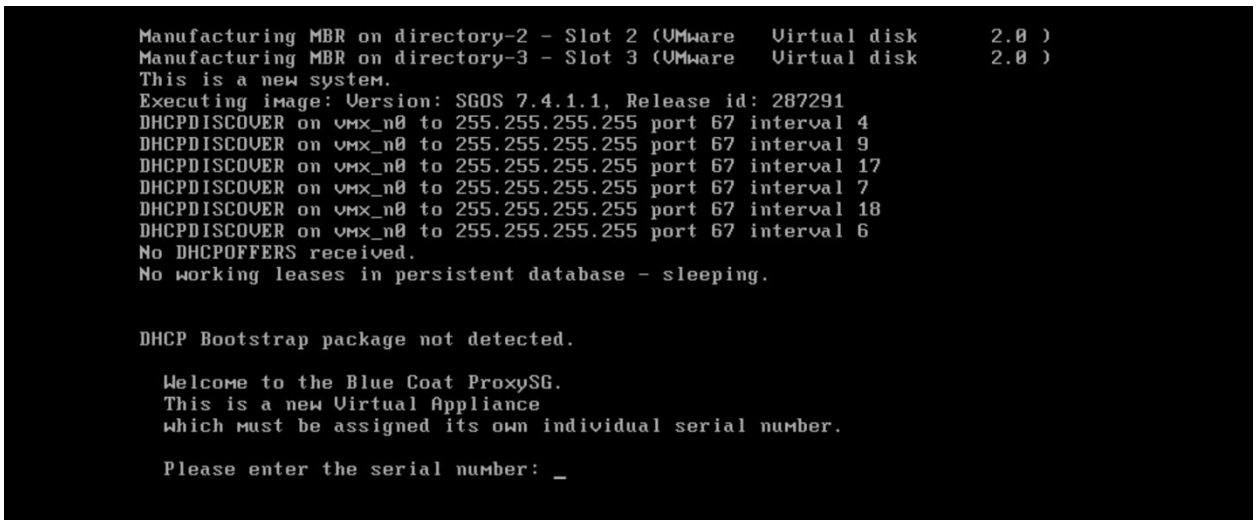

Рис.3.7. Введення серійного номеру.

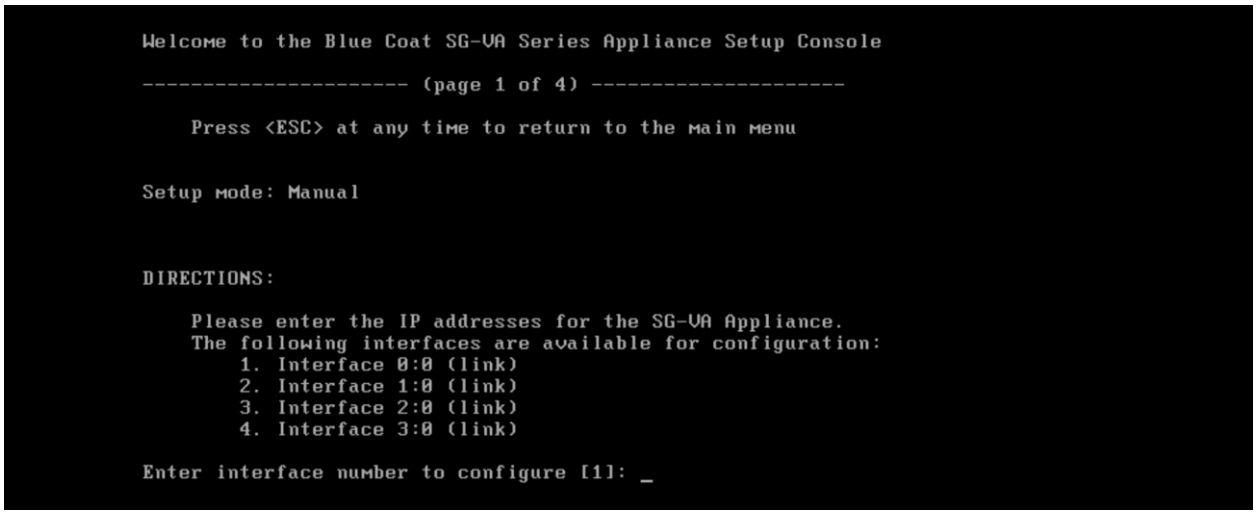

Рис.3.8. Введення мережевих параметрів.

3.2. Проектування бази даних

Для інтеграції деяких рішень, навіть декількох модулів не достатньо розгорнути лише appliance, потрібно додатково інсталювати додаткові модулі, які будуть взаємодіяти з усією системою повністю.

В даній роботі рішення Fudo PAM використовує вбудовану БД для роботи системи в цілому і від адміністратора системи не потребує додаткових налаштувань чи додаткових компонентів, модулів для роботи системи.

Якщо аналізувати рішення від Fidelis EDR, то інсталяція потребує додатковий компонент у вигляді БД Microsoft SQL, яка в собі буде містити

данні про користувачів, які присутні в системі. Основна ціль рішення це контроль за кінцевими робочими станціями користувачів, за допомогою агентів, які встановлюються на робочі станції та дають повну видимість дій користувачів, запущених процесів.

Для того щоб розгорнути БД потрібно використати SQL Server Installation Center, рис.3.9-3.10.

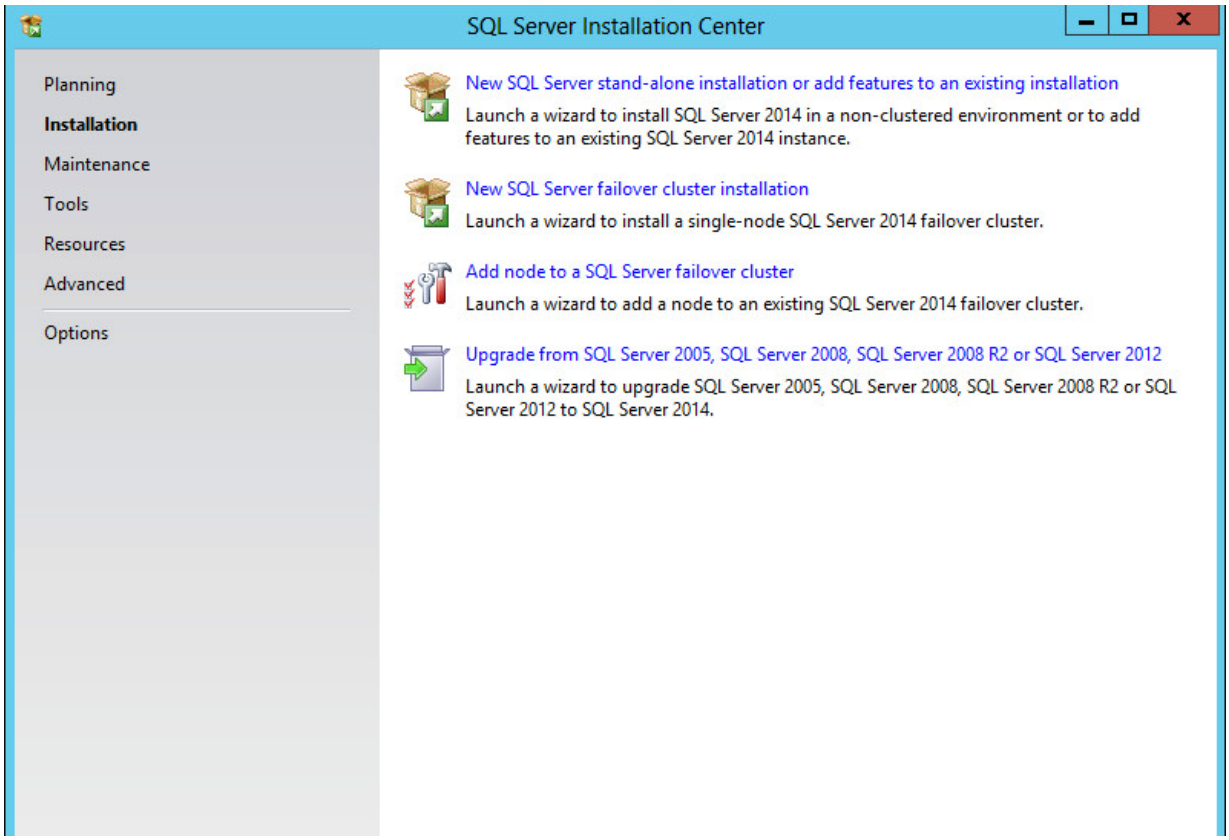

Рис.3.9. SQL Server Installation Center.

Після проходження процесу інсталяції бази даних, потрібно додатково інсталювати MS Management Center, звідки є можливість здійснювати адміністрування БД та перегляд інформації в ній. Створена база даних матиме відповідну до рис.3.10, структуру.

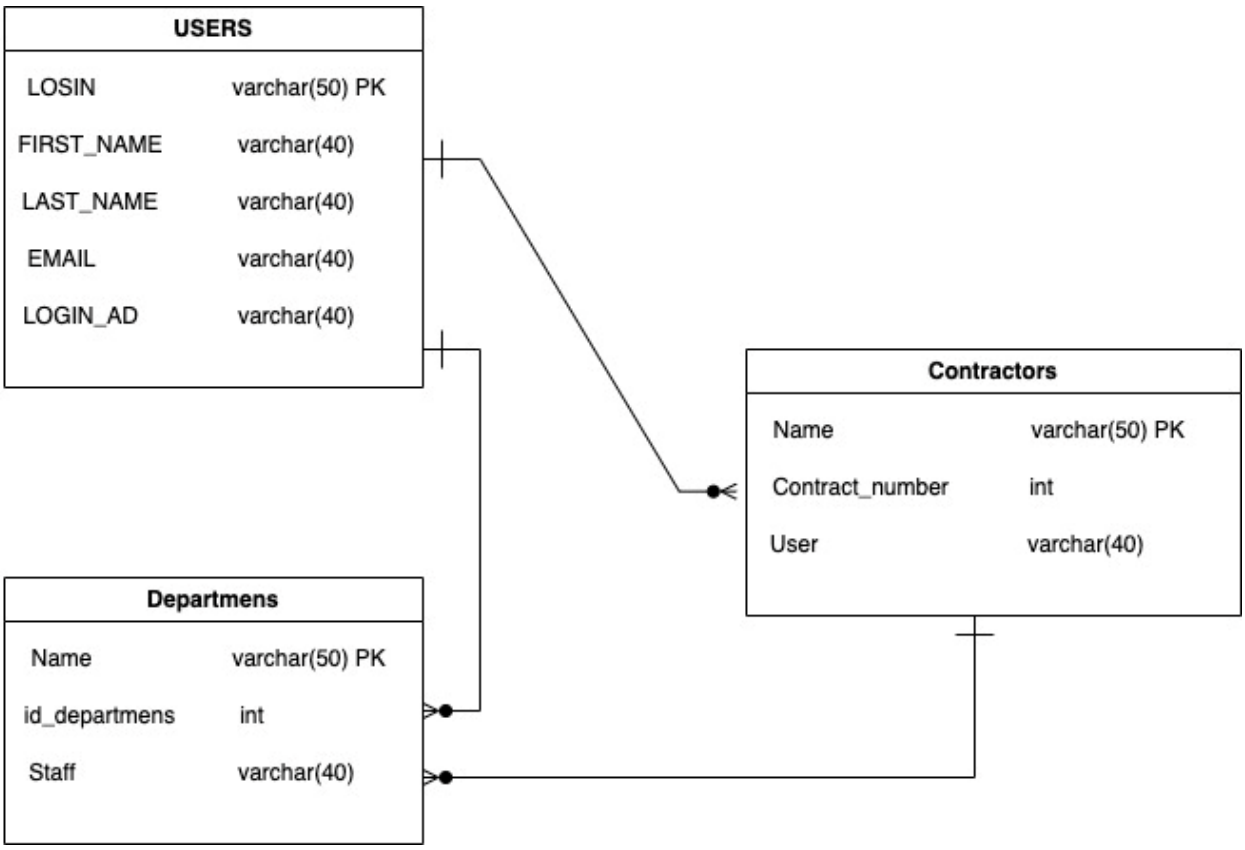

Рис.3.10. Архітектура бази даних.

3.3. Початок роботи з Fudo PAM

Після того, як було розгорнуто рішення, та активована ліцензія, система дає змогу продовжити роботі по інтеграції системи до еко-системи компанії. Перш ніж приступити проводяться аналітичні комунікації з замовником, для визначення архітектури побудови рішення. Це мається на увазі, що як буде побудована відмовостійкість системи, як буде відбуватися підключення до цільових систем. Можливо є необхідність в додатковому розроблені функціонала, наприклад, підключення до термінальних ферм, які мають складний механізм підключення тобто присутність балансеру. Ці дії виконуються для того щоб зробити підключення користувачів простим та зручним.

3.3.1 Інтеграція с Active Directory

Під час впровадження основною задачею для полегшення авторизації користувачів, було виконано інтеграцію з «Active Directory», дана дія дає змогу автоматизовано здійснити синхронізацію користувачів, які знаходяться в корпоративному домені, та оптимізувати роботу адміністратора системи, щоб не заводити локально користувачів. В той же час користувачам також буде простіше пройти автентифікацію на порталі користувача та здійснювати підключення до цільових систем з нього.

Інтеграція відбувається в два етапи налаштування «Автентифікації» та «Синхронізація з LDAP»

«Синхронізація з LDAP» відбувається наступним чином: надання назви, встановлення пріоритету, а далі заповнення відповідних полів які є обов'язковими. Єдине потрібно обрати тип сервера в роботі це Active Directory. Щоб усе запрацювало потрібно на мережевому рівні надати відкритий порт 636 або 389 в залежності від мережевої інфраструктури замовника. В роботі побудовано на порту 636.

На рис.3.11-3.14, видно, як проходить інтеграція.

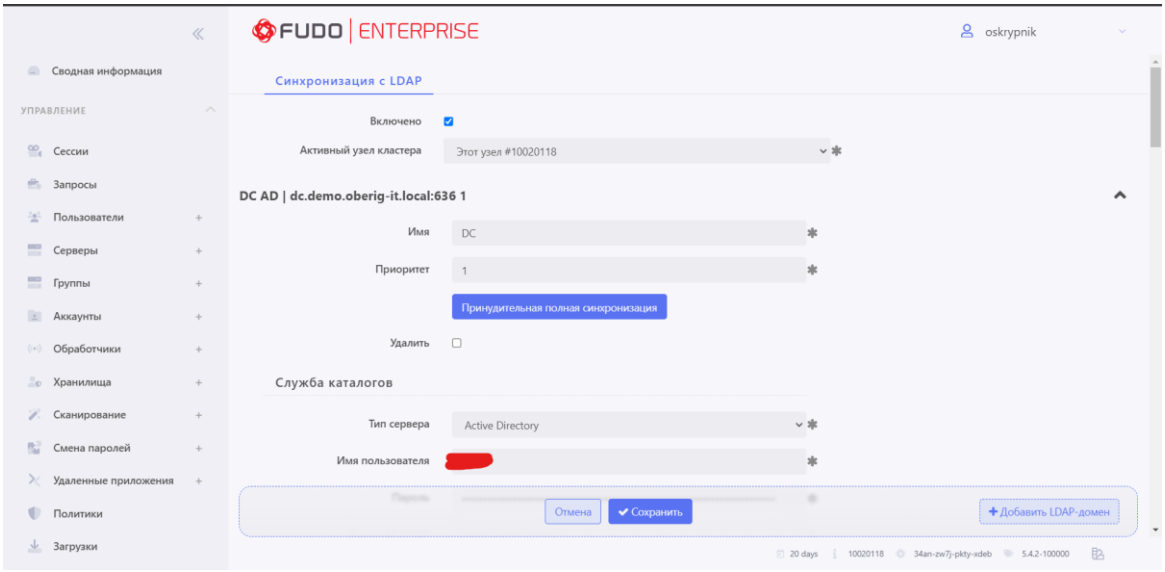

Рис.3.11 Інтеграція LDAP.

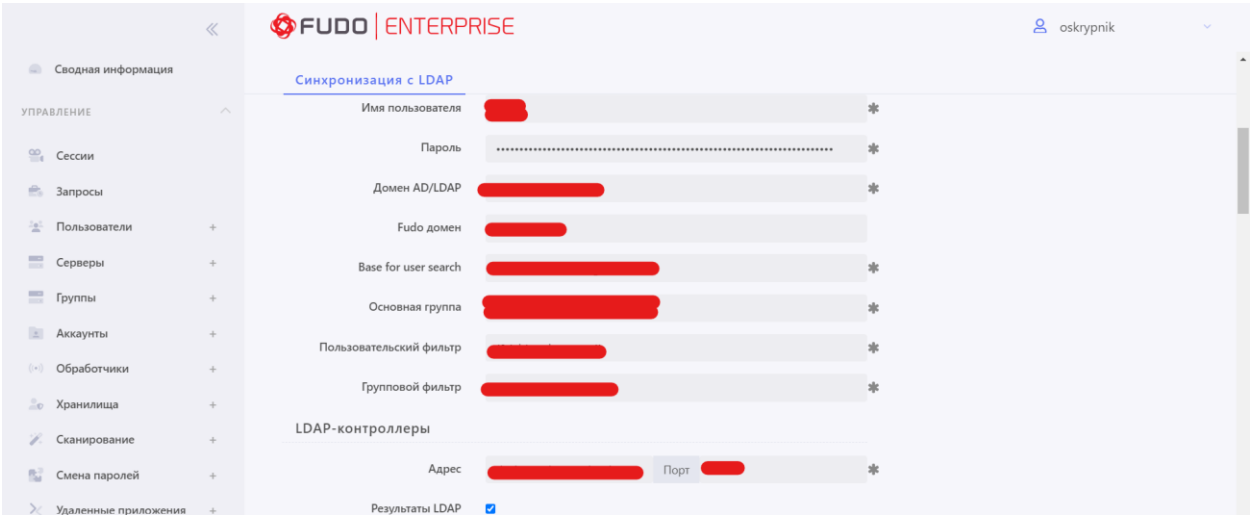

Рис.3.12. Інтеграція LDAP.

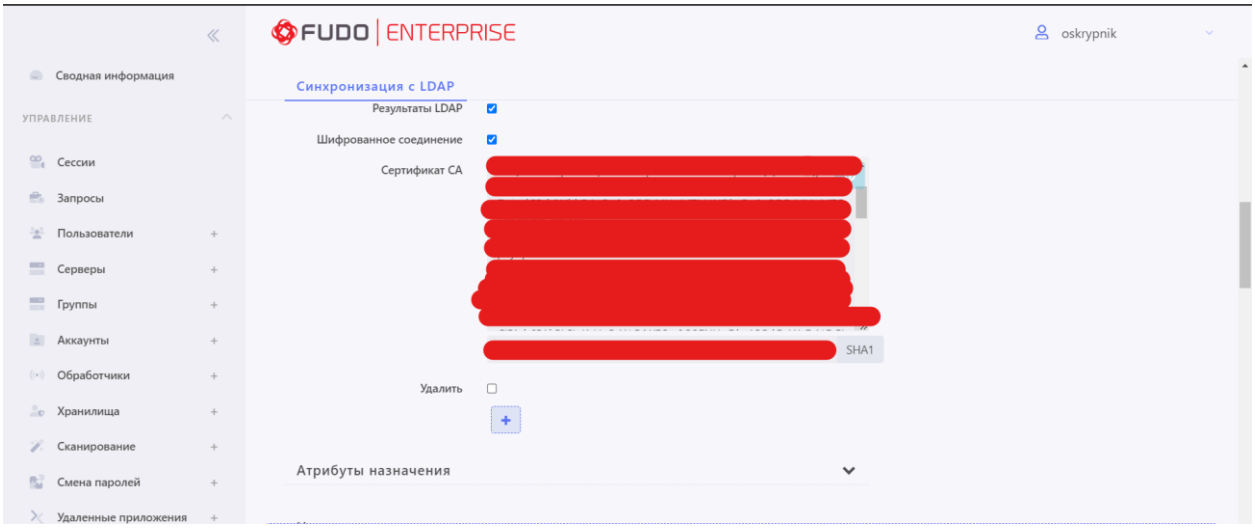

Рис.3.13. Інтеграція LDAP.

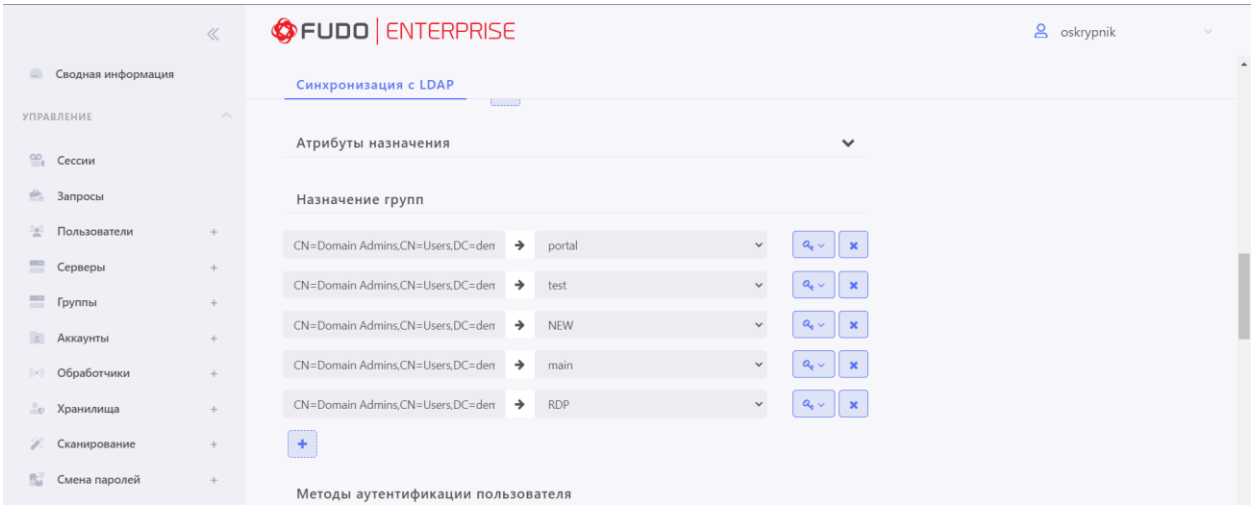

Рис.3.14. Інтеграція LDAP.

3.3.2. Організація підключення, до цільової системи

Була виконана конфігурація з налаштування підключення до цільової системи. Сконфігуровано «Server», де буде обрано протокол за, для підключення та прив'язки IP-адреси до «appliance», Fudo, рис.3.15.

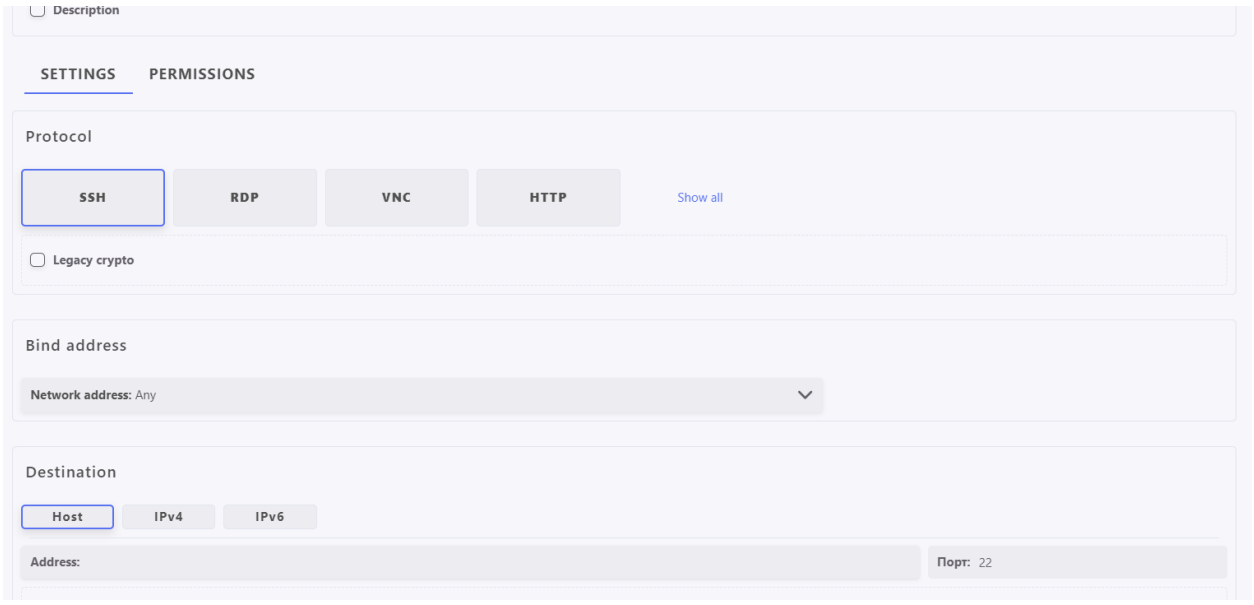

Рис.3.15. Меню налаштування «server».

Після того, як було здійснено налаштування для «Server», було налаштовано меню «Account» визначення логіну на паролю для авторизації користувачів. Це реалізується шляхом налаштування типу «прокидання» (anonyms, forward, regular). Додатковим параметром буде активація запису сесії тобто увімкнення механізму «OCR», який підтримує всі мови інтерфейсу. Налаштування «account» рис.3.16-3.17.

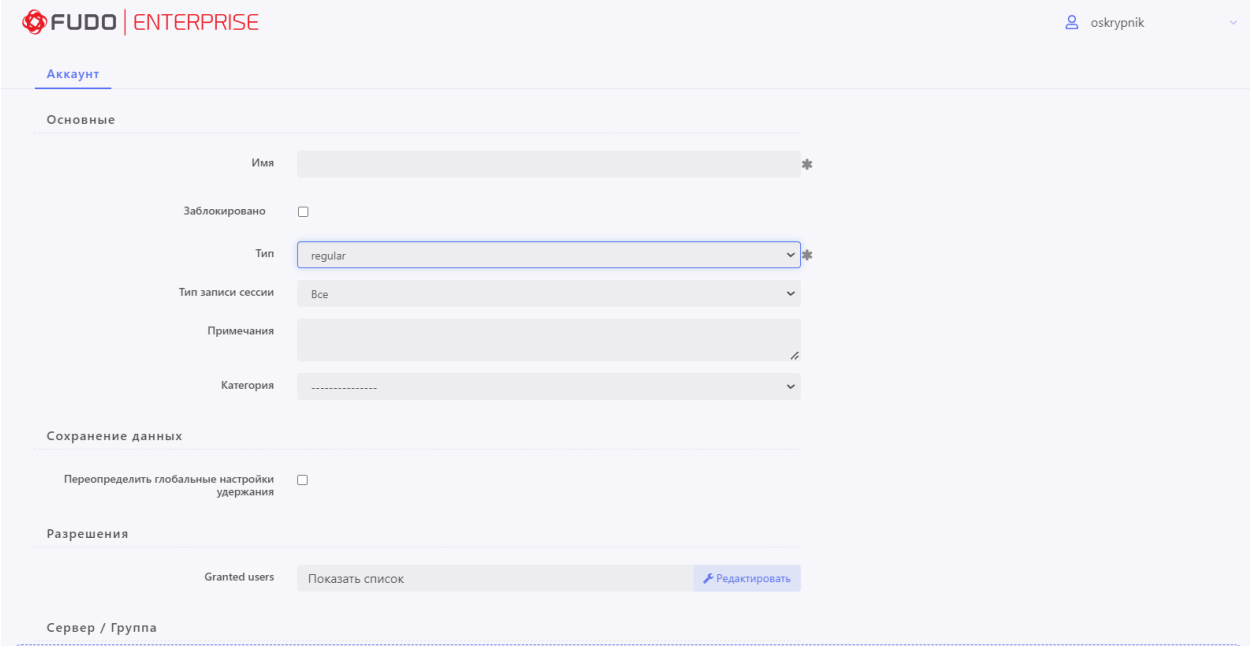

Рис.3.16. Налаштування «account».

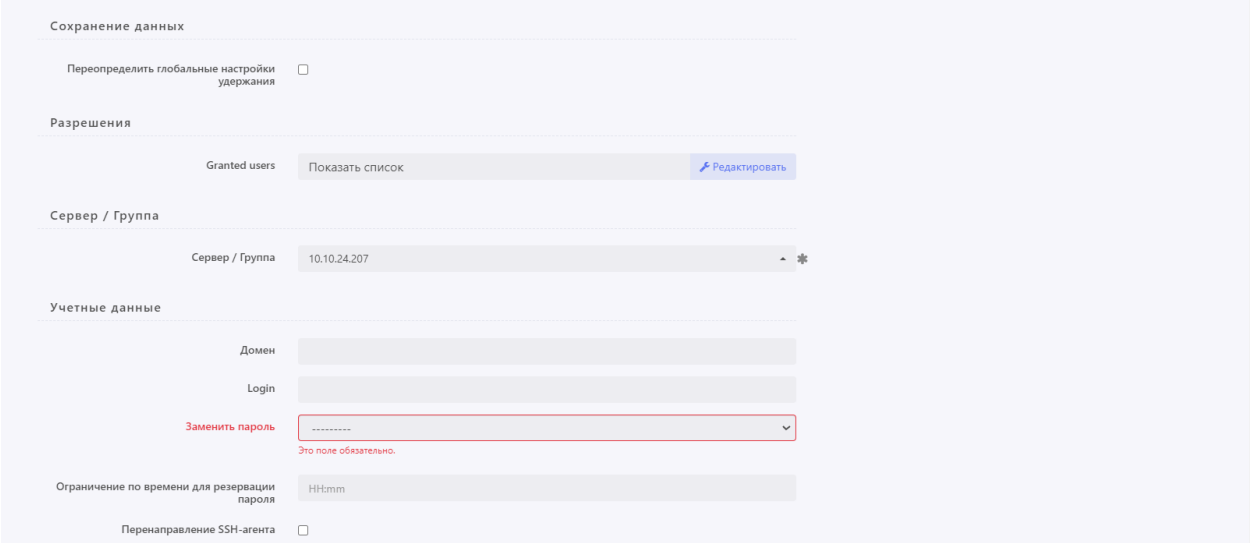

Рис.3.17. Налаштування «account».

Для підключення здійснено налаштування ще двох пунктів, а саме «listener» та «safe».

Listener – необхідний для налаштування підключення до цільової системи через Fudo (proxy, bastion, bridge, gateway).

Safe – потрібний для того щоб об’єднати всі попередні налаштування та додати певні налаштування, якщо вони є необхідними.

Налаштування «listener» та «safe» представлені на рис.3.18-3.19.

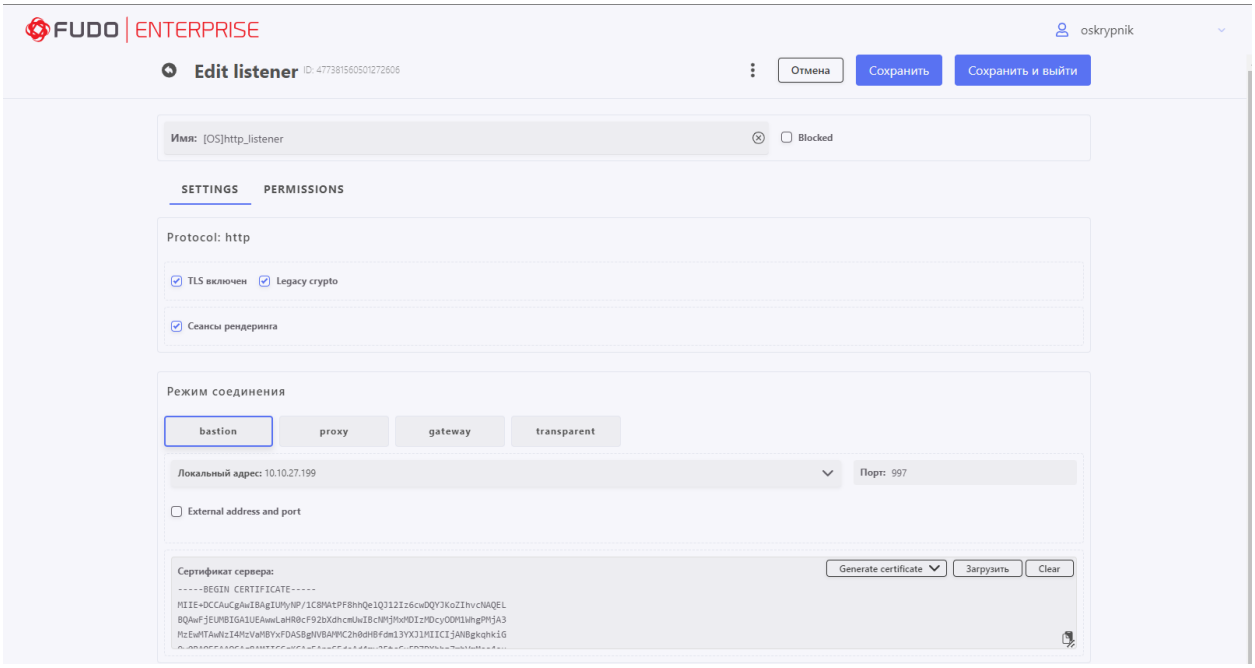

Рис.3.18. Налаштування «listener».

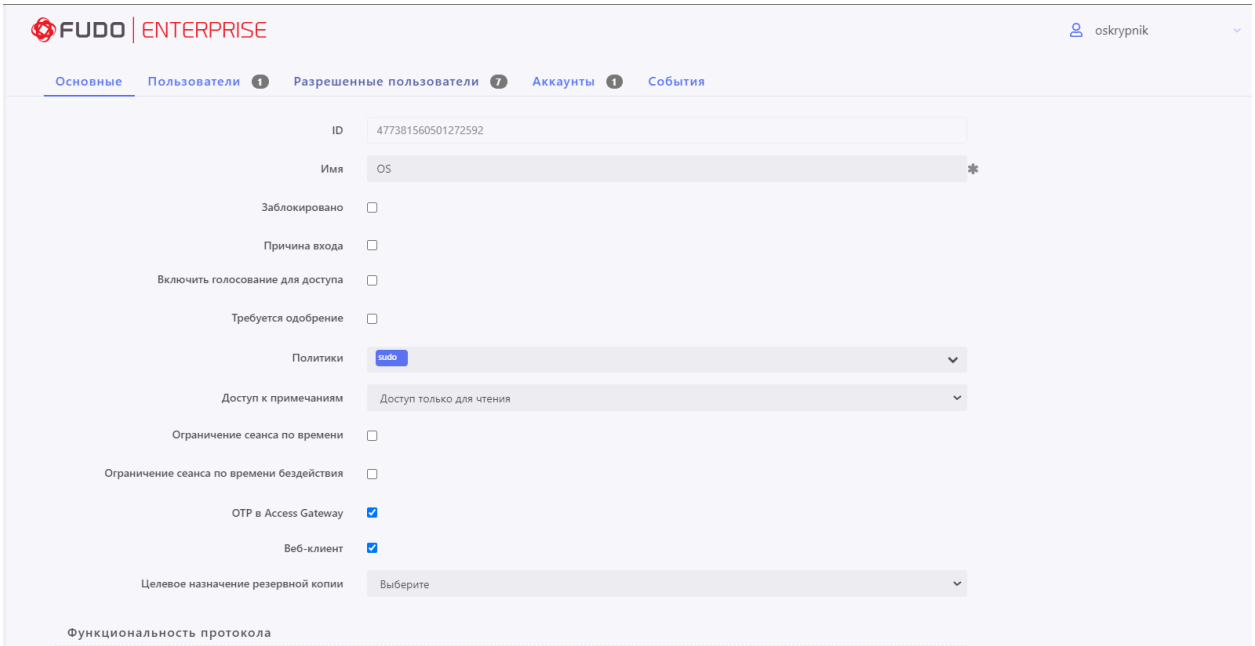

Рис.3.19. Налаштування «safe».

3.3.3. Налаштування політик

Налаштування політик є необхідним функціоналом в даному сегменті систем. Політики безпеки дозволяють здійснювати контроль за діями користувачів в автоматизованому режимі. Це реагування на введення команд з клавіатури. В Fudo PAM, правила пишуться на основі регулярних виразів, які представлені в форматі коду, який здійснює реагування на текст для пошуку та реагування на даний текст відповідними діями. Даними радикальними діями, може бути блокування користувача або закінчення сесії, а якщо дана сесія була погоджена запитом адміністратором, то при її розтермінувані потрібно буде здійснювати надсилання запиту адміністратору на погодження. В роботі було розроблено ряд політик для спрацювань.

Написання регулярних команд рис.3.20.

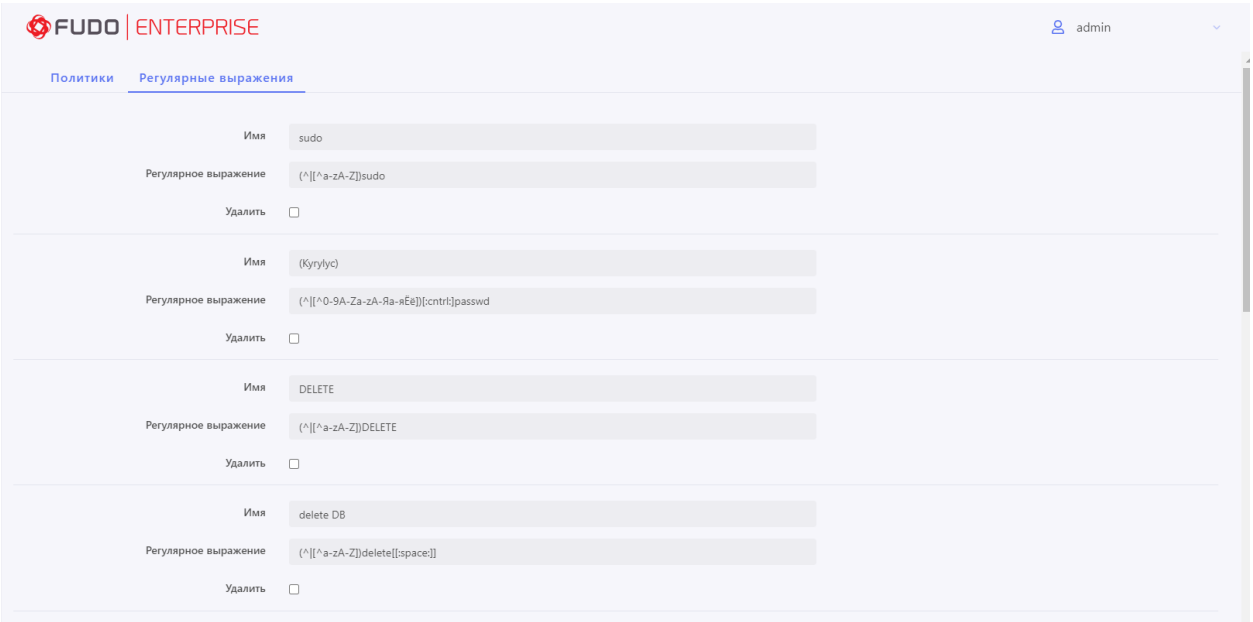

Рис.3.20. Написання регулярних виразів.

3.3.4. Відпрацювання рішення Fudo PAM

Для підключення до цільової системи, користувач може використовувати, як нативний клієнт так і користувацький портал.

Користувач може відправляти запит на підключення з користувацького порталу, що зменшує документообіг в організації. Можна виставити кількість користувачів «адміністраторів», які повинні погоджувати надання доступу до цільової системи. Адміністратору не має необхідності при цьому здійснювати підключення до адміністративного порталу, це зробити можна через мобільний додаток.

Процес підключення та надсилання запиту з користувацького порталу зображено на рис.3.21-3.22.

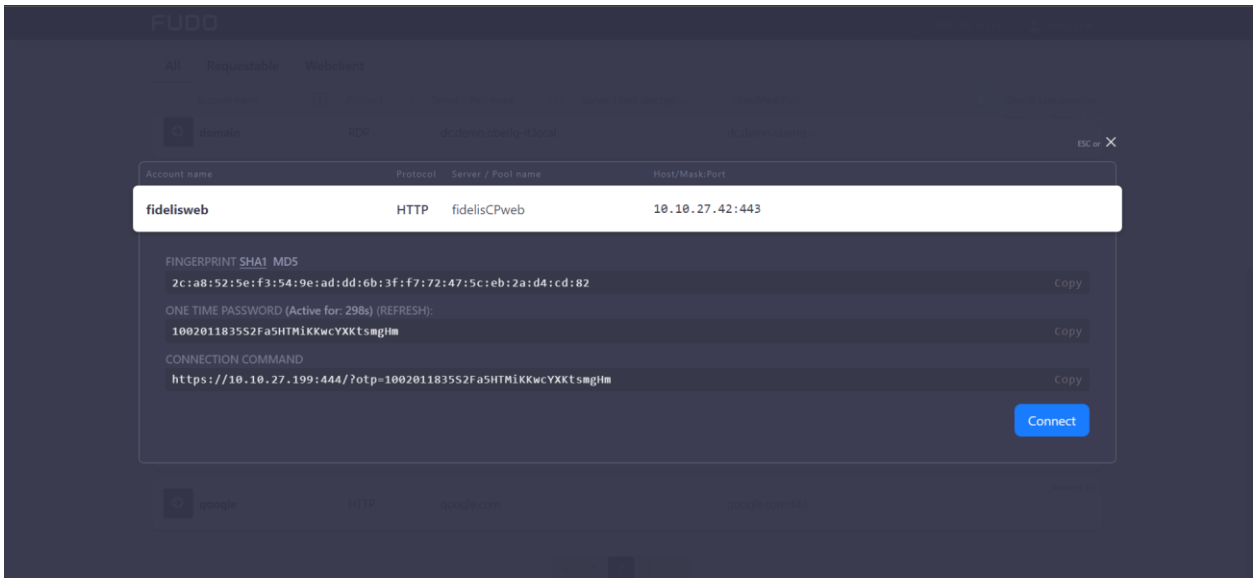

Рис.3.21. Початок підключення до цільової системи.

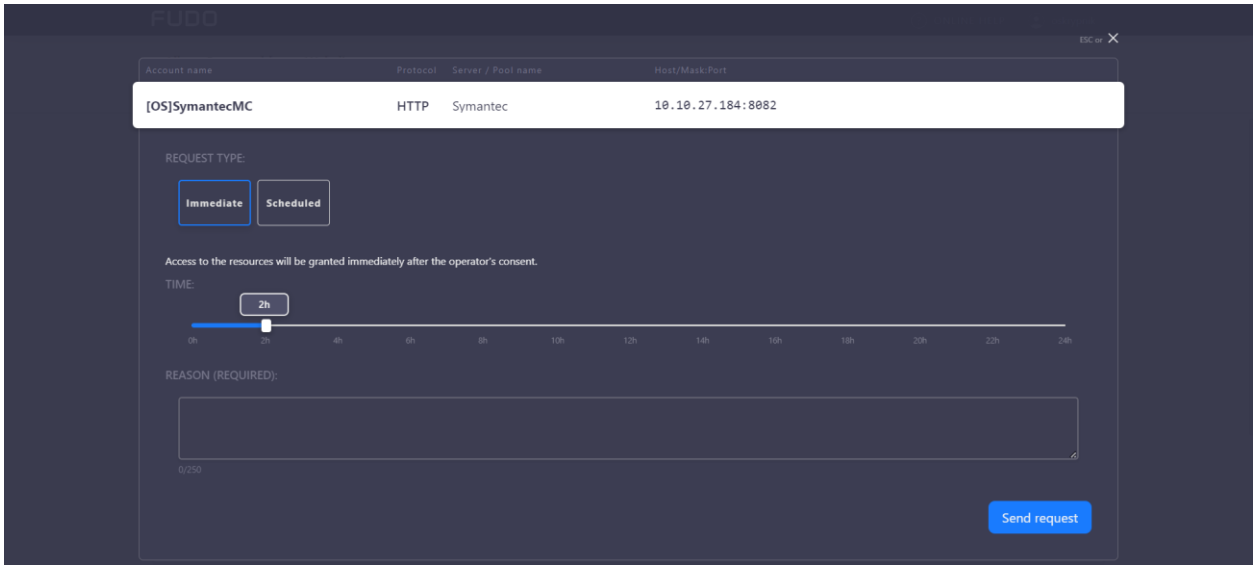

Рис.3.22. Надсилання запиту на підключення.

З боку адміністратора на порталі адміністратора системи це виглядатиме наступним чином, рис.3.23-24.

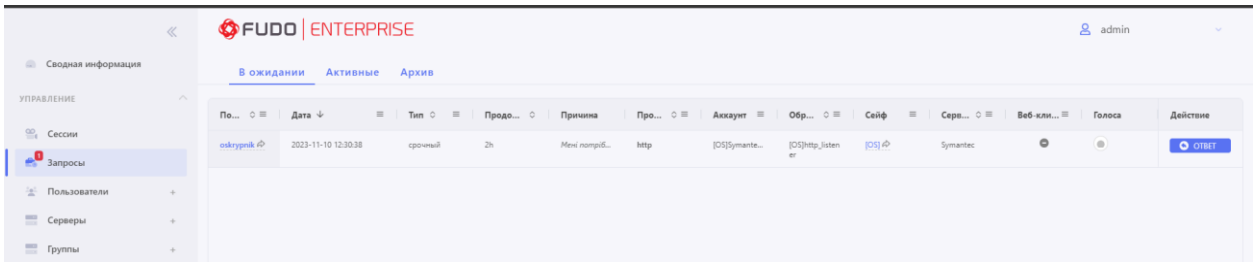

Рис.3.23. Запит на підключення на адмін порталі.

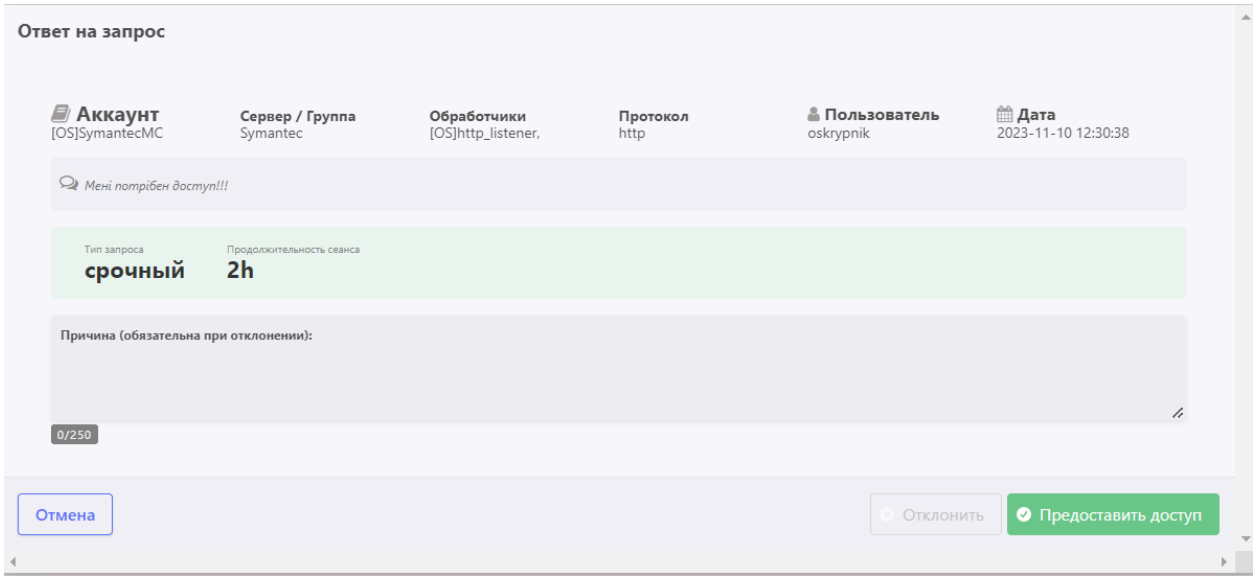

Рис.3.24. Опис запиту.

У користувача буде відкрите нове вікно в браузері, через яке зможе працювати з системою, рис.3.25.

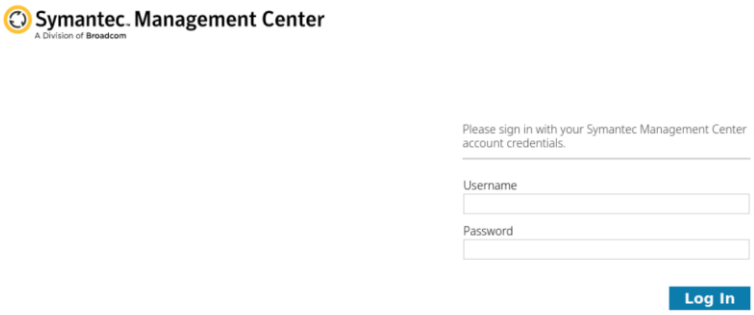

Рис.3.25.Користувацька сесія.

Адміністратор може в реальному часі переглядати сесію ініційовану користувачем та переглядати дії та вводимі команди, а також підключатися до неї віддалено та навіть розтермінувати сесію.

Інтерфейс адміністратора рис.3.26.

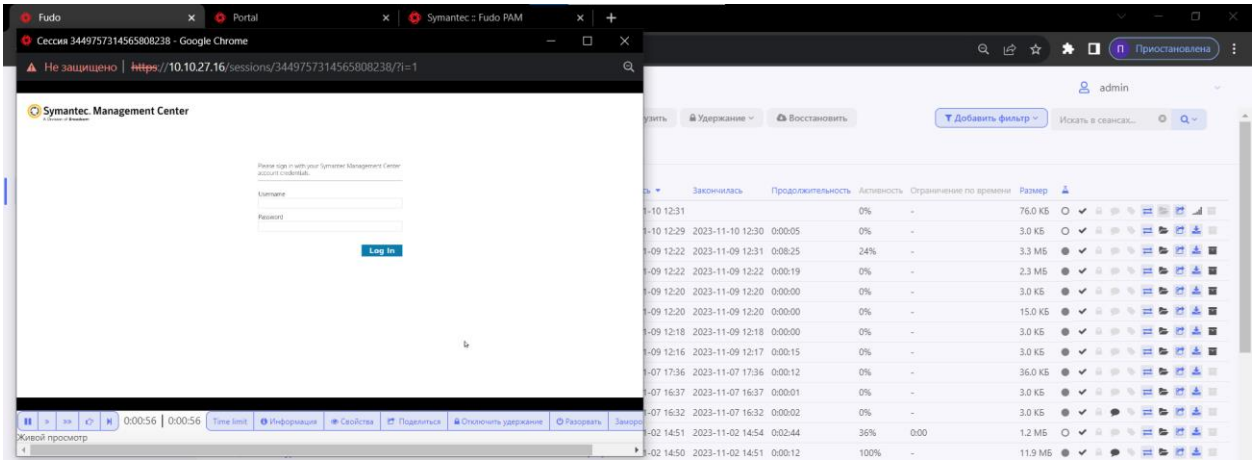

Рис.3.26. Перегляд сесії користувача.

3.4. Початок роботи з WSS Symantec

Для початку роботи потрібно розгорнути WSS Symantec на обраному віртуальному середовищі, встановленому у замовника. В даній роботі всі віртуальні appliances розгорнуті на VMware. Оскільки рішення багатомодульне, і включає в себе розгортання не лише одного appliance, а декількох модулів для повноцінної функціональності системи, в роботі розгорнуто два proxy сервера, які працюють в форматі кластеру (active-passive), консолі управління, reporter та content analysis system.

Після того як всі віртуальні appliances були розгорнуті, вони мають окремі веб-інтерфейс для їх взаємодії, але адміністрування можна проводити централізовано в одному місці консолі управляння (management center). В ньому можна робити кастомізацію всього рішення та здійснювати розповсюдження політик на всі proxy сервери, які є в кластері. Щоб це зробити потрібно додати всі модулі в консоль управляння, що було зроблено та можна побачити на рис.3.27.

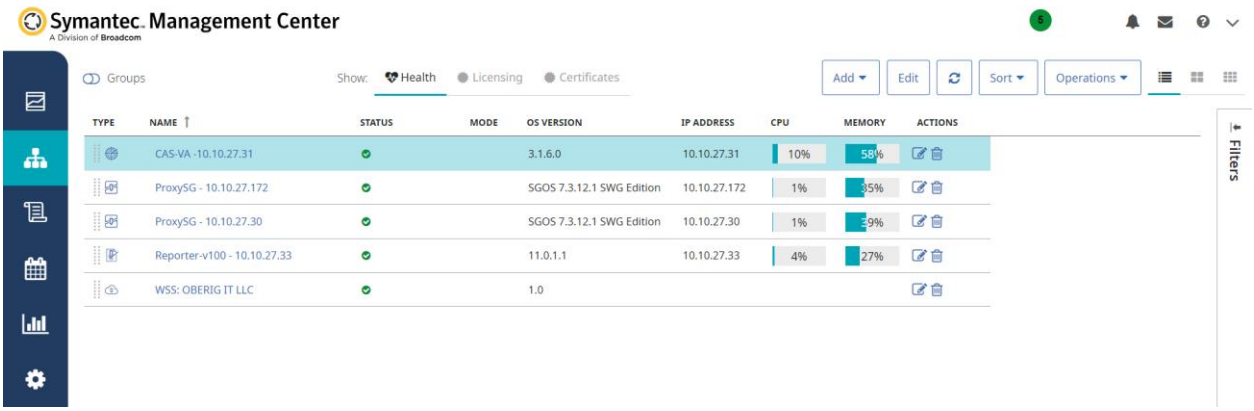

Рис.3.27. Список всіх доданих модулів.

Після того, як всі модулі додані в консолі управління, можна передивлятися статичну інформацію в форматі (health check), на початковій сторінці (dashboard), рис.3.28.

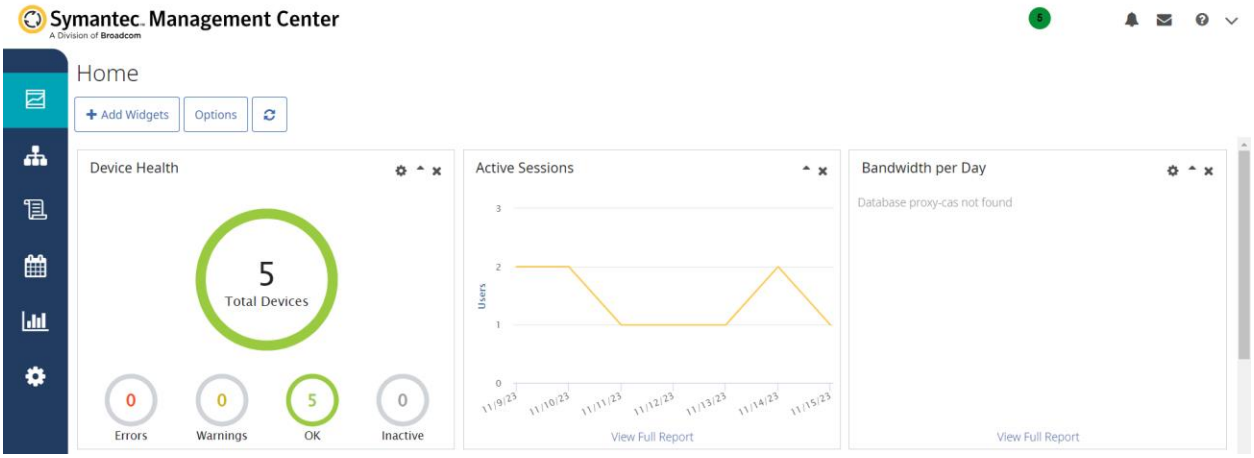

Рис.3.28. Dashboard.

Стосовно кастомізації та створення глобальної розсилки політик, потрібно використати вбудований інтерфейс Policy objects, рис.3.29.

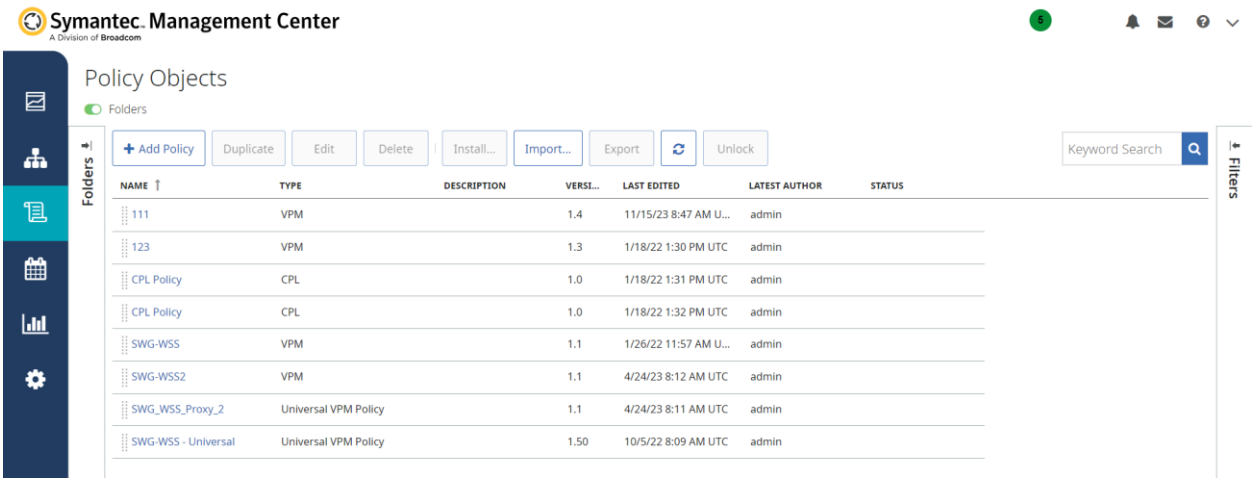

Рис.3.29. Policy objects.

Для автоматизації роботи при побудові кластеру було розроблено кастомний скрипт, за допомогою, якого буде відбуватися імпортування політик на обраний proxy сервер (рис.3.30).

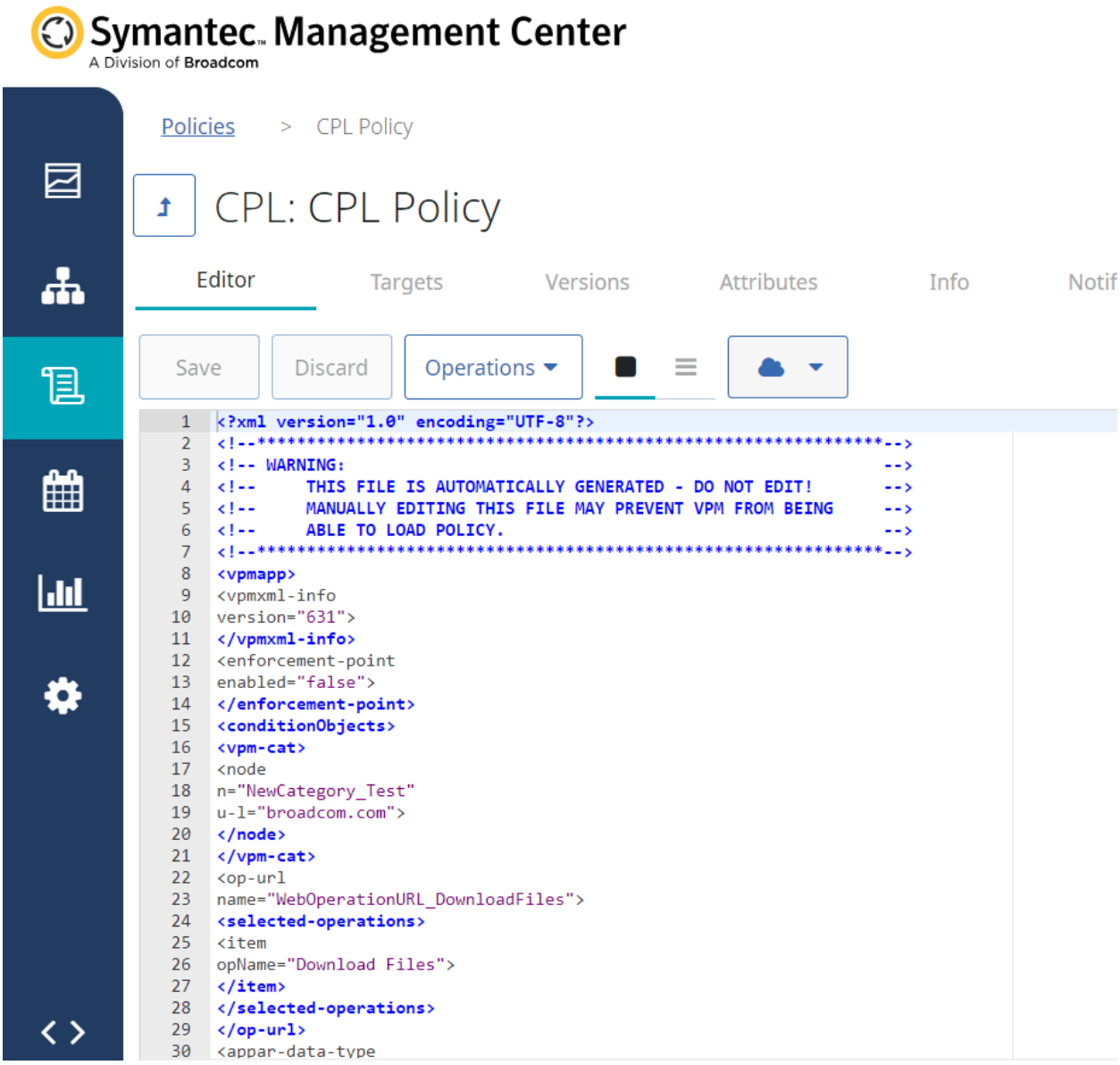

Рис.3.30. Скрипт для імпорту політик.

3.4.1 Робота з Proxy сервер

Основним модулем, з яким відбувається взаємодія адміністратора це proxy сервер. Тому що саме proxy сервер виконує прокусування (пропускання через себе трафік) через себе трафік, який надходить від користувачів за периметр організації.

Саме на proxy сервер, відбувається налаштування політик, які будуть опрацьовувати запити користувачів та реагувати на них відповідними діями. Після того, як відбудеться спрацювання політики, статистика направляється на аналіз до CAS (content analysis system), де за потреби буде на правлений в sandbox, для його більшого дослідження. На додаток є вбудований антивірусний захист, який також розбирає отримані файли користувачем.

Proxy сервер також виконує функції блокування ресурсів не лише як окремі url-сторінки, а й повністю відповідно до категорій до яких вони відносяться.

Proxy сервер має власний веб-інтерфейс для адміністрування, де можна переглянути статистику роботи модуля та підключення користувачів через Proxy сервер, рис 3.31-32.

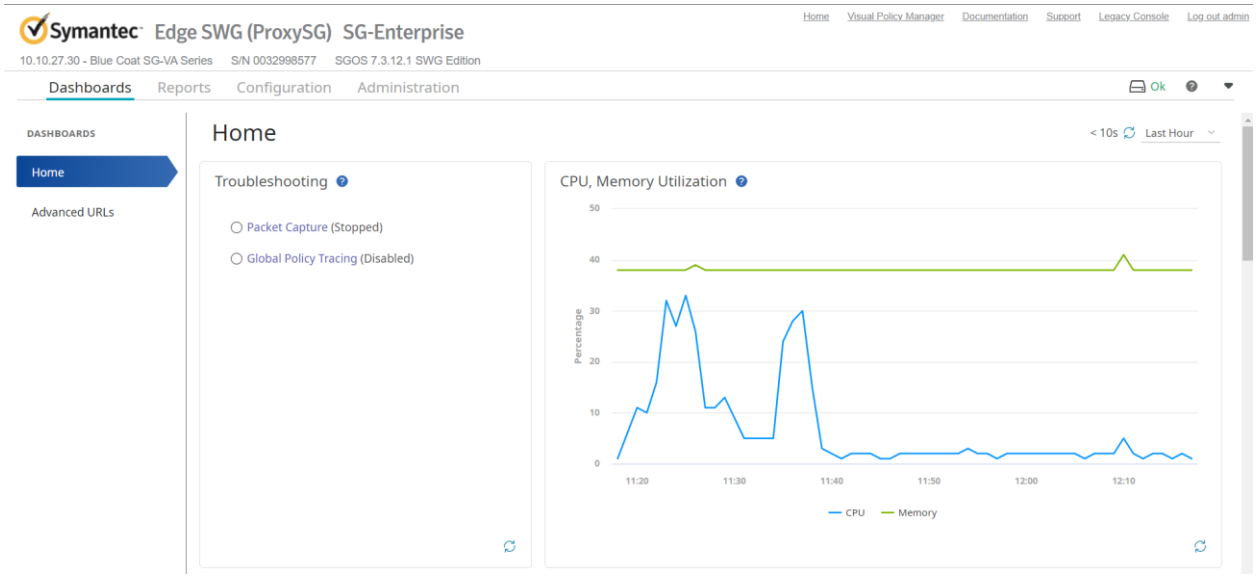

Рис.3.31. Статистика роботи модуля Proxy сервер.

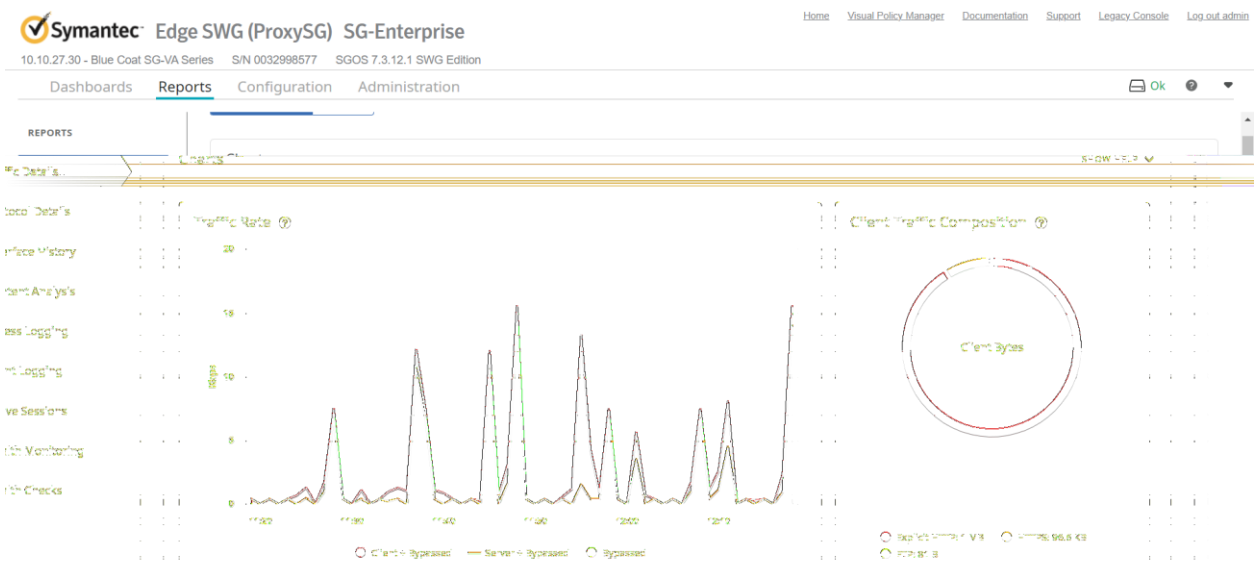

Рис.3.32. Статистика підключення до модуля Proxy сервер.

Налаштування політик, відбувається в окремому веб-інтерфейсі, під час виконання розробки даного рішення було розроблено ряд політик, як базові так і на вимогу замовника рис.3.33.

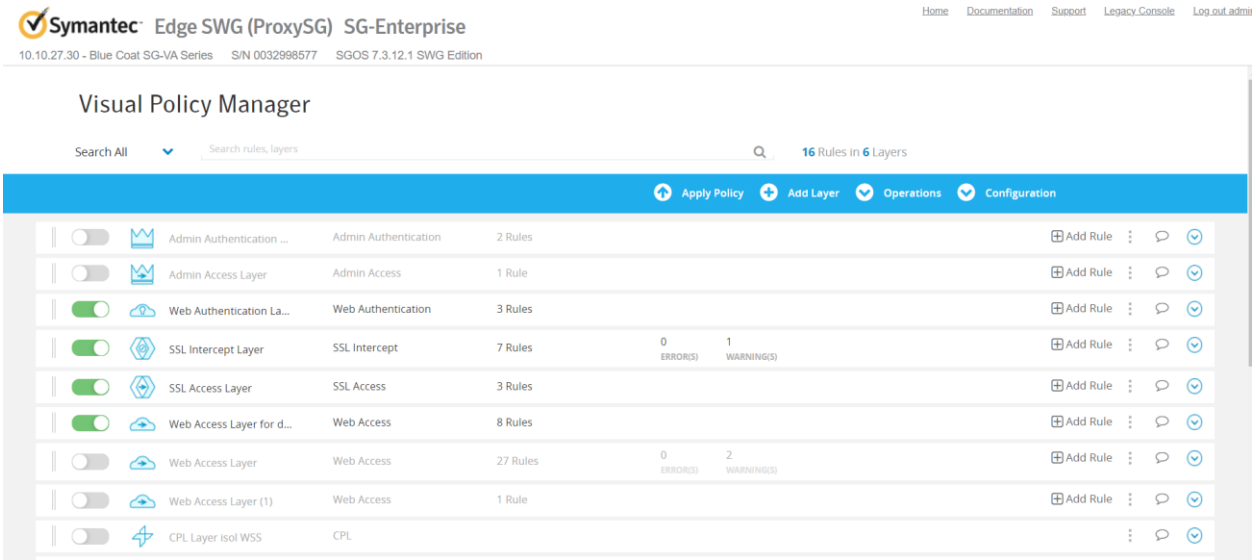

Рис.3.33. Налаштування політик на Proxy сервер.

Користувач побачить сторінку, яка попередить що спрацювала політика Proxy сервера. Дану сторінку відображення спрацювання, можна кастомізувати за допомогою коду HTML.

Стандартна сторінка відображення спрацювання має наступний вигляд рис.3.34

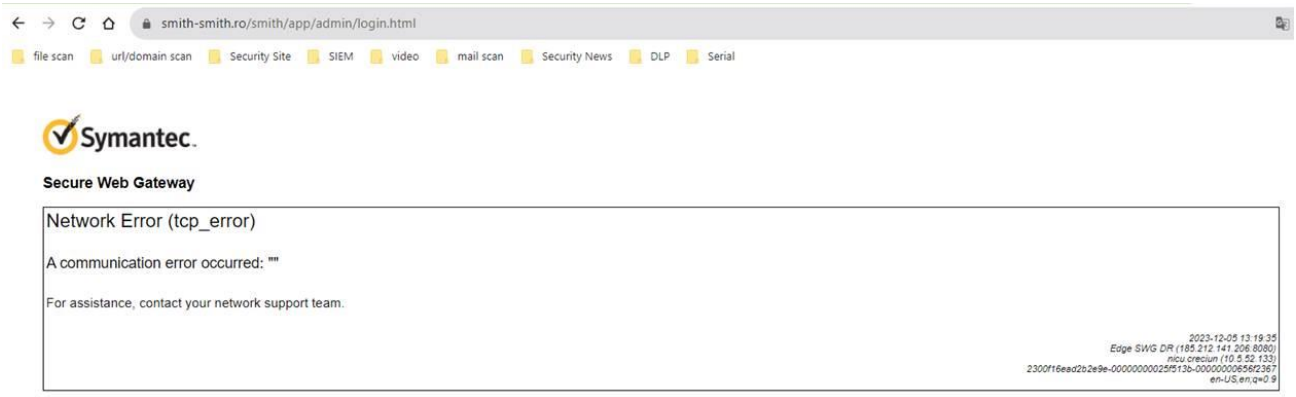

Рис.3.34. Спрацювання політики Proxy сервер.

3.5. Початок роботи з EDR Fidelis Network та Endpoint

Всі рішення такого класу потребують передусім розгортання всіх модулів та заведення в єдину систему для локального адміністрування з однієї консолі. Якщо дивитися попередні рішення то кожен модуль мав окремий веб-інтерфейс за допомогою, якого можна здійснювати адміністрування окремого модулю. В даному випадку з Fidelis, як платформи в цілому такої можливості є консоль управління одна, яка поєднує в собі Network та Deception, та окремий веб-інтерфейс Network.

Стандартно, як і в попередніх рішеннях перше, що буде бачити адміністратор, це Dashboard, де відображається статистика з компонентів, які виводить система, рис.3.35.

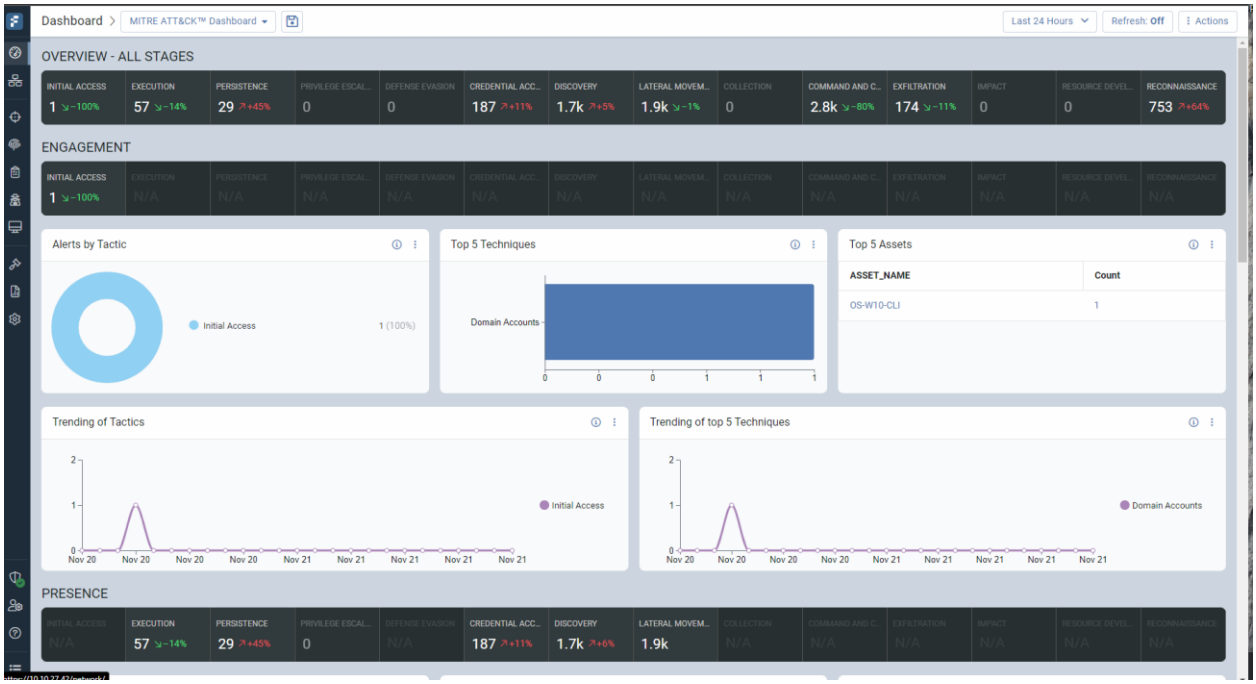

Рис.3.35. Dashboard Fidelis.

Окремим цікавим інтерфейсом, є змога побудови топології мережі, за допомогою, механізму опитування системою пристроїв. Тобто в орієнтовному проміжку часу, а це кожні 5 хвилин здійснюється змога підключитися до агенту, який встановлюється на робочу станцію та перевірка з'єднання. На основі цього рішення може будувати топологію мережі а також її редагувати, якщо певна робоча станція є недоступною, рис.3.36.

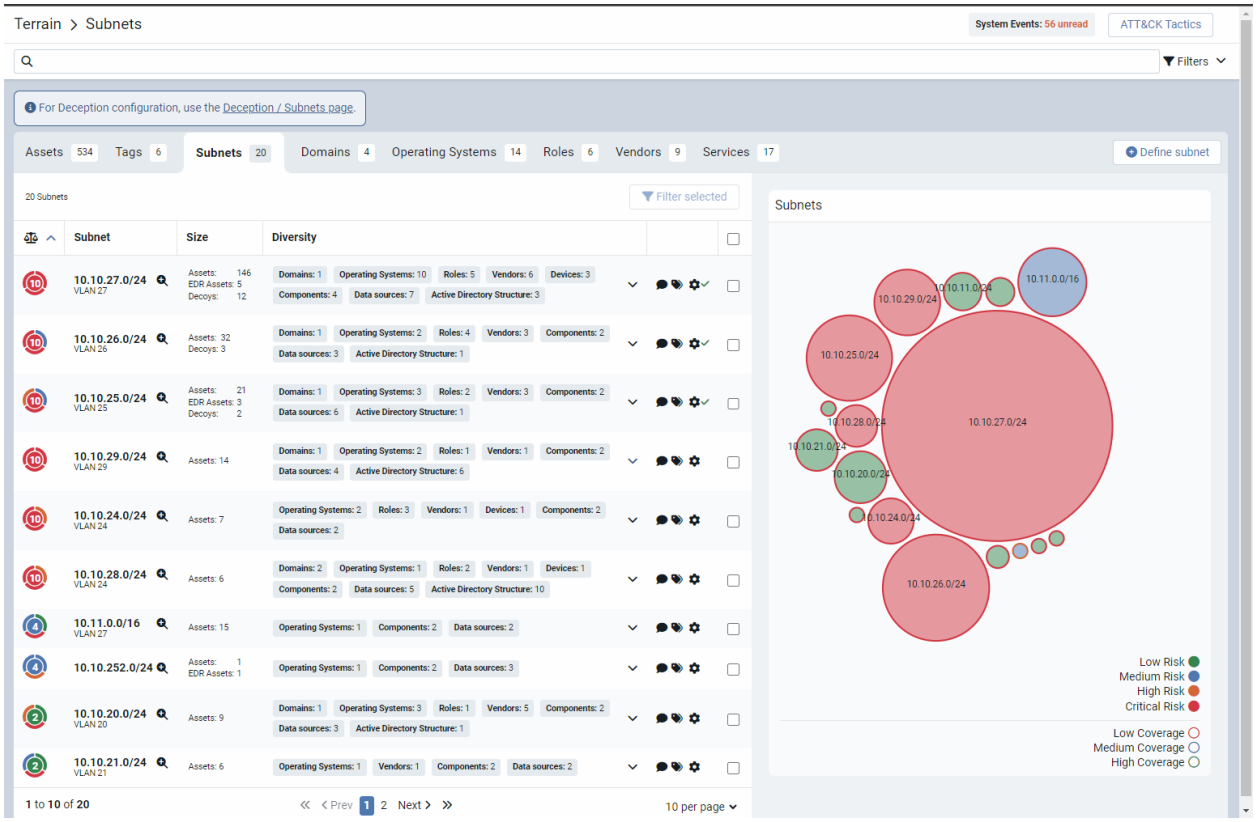

Рис.3.36. Топологія мережі за допомогою Fidelis.

З даного зображення можна побачити підмережі, які присутні в організації та ознайомитися з інформацією, такою, як кількість пристроїв в підмережі, вид пристрою (сервера, робочі станції користувачів).

Для більш детальної інформації, яка надається системою, використовують сенсори, які розгортаються, паралельно до продуктивної мережі, і налаштовують дзеркальований трафік, тобто система аналізує копію трафіку, що забезпечує швидке підключення та для користувачів не помітні затримки.

Для коректної роботи рішення було здійснено налаштування дзеркалювання трафіку, що дає змогу за допомогою вбудованих механізмів розбирати трафік, як вхідний так і вихідний та аналізувати і надавати інформацію по ньому, рис.3.37-3.38.

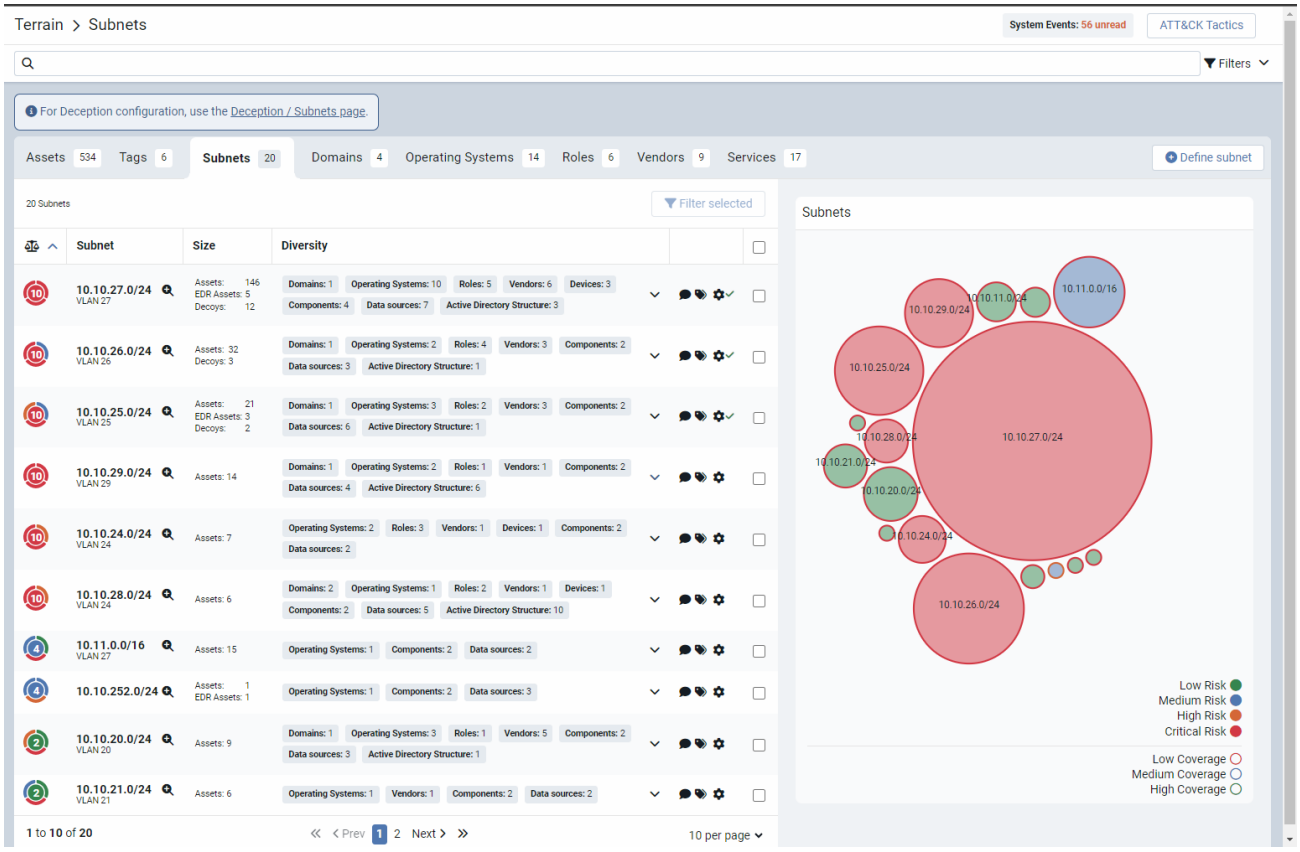

Рис.3.37. Розбір трафіку за допомогою сенсорів Fidelis.

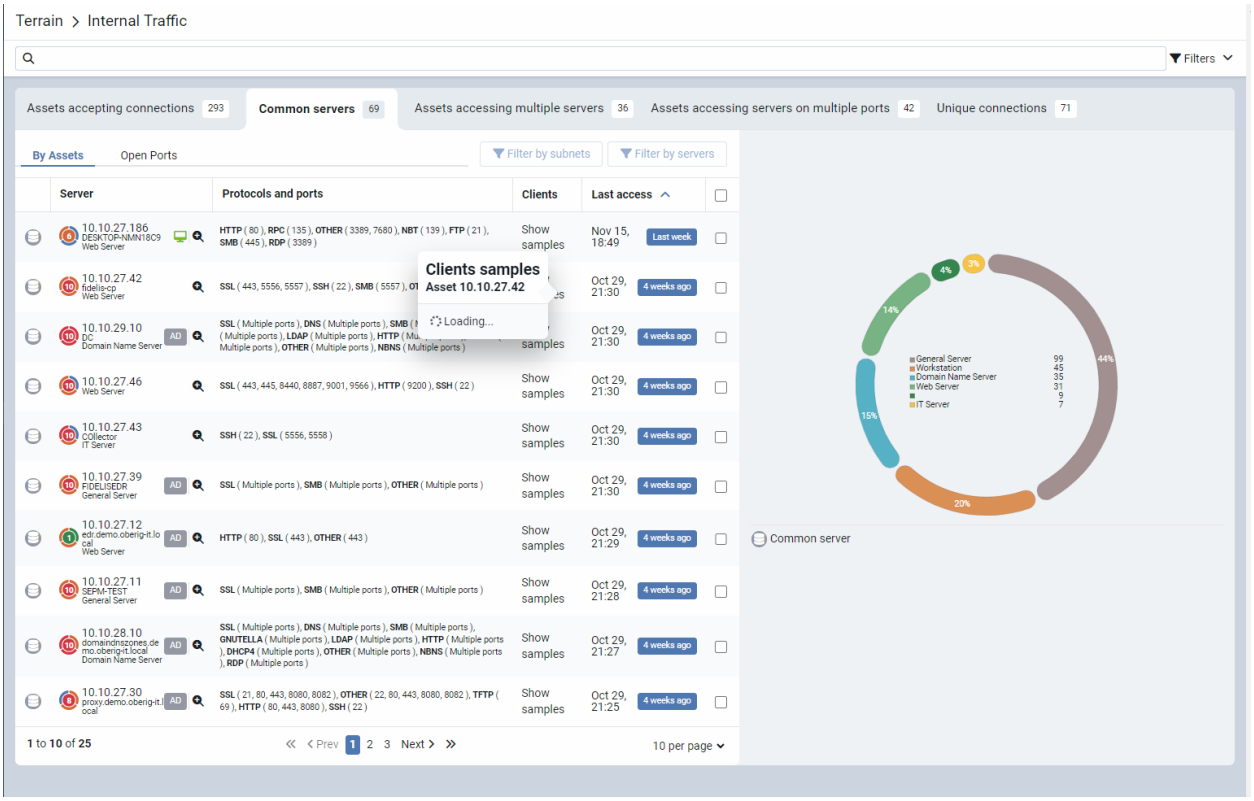

Рис.3.38. Розбір трафіку за допомогою сенсорів Fidelis.

Головним завданням є розробка пасток (Decoys) та «хлібні крихти» (Bread crams).

Дана можливість дає змогу ввести в оману зловмисника, що зможе подумати, що дана пастка є цільовою системою, на яку він полює. Пастки розгортаються, як реальні системи в підмережах навіть можна обрати тип даної пастки (ПК, веб-камера, сервер).

Розгорнуто достатню кількість пасток, що здійснюють комунікацію між собою та імітують активність в мережі. Хлібні крихти також були створенні для того щоб заманити зловмисника на пастку – це певні файли, які були підготовлені, та журнали.

На рис.3.39, можна побачити результат розгортання пасток.

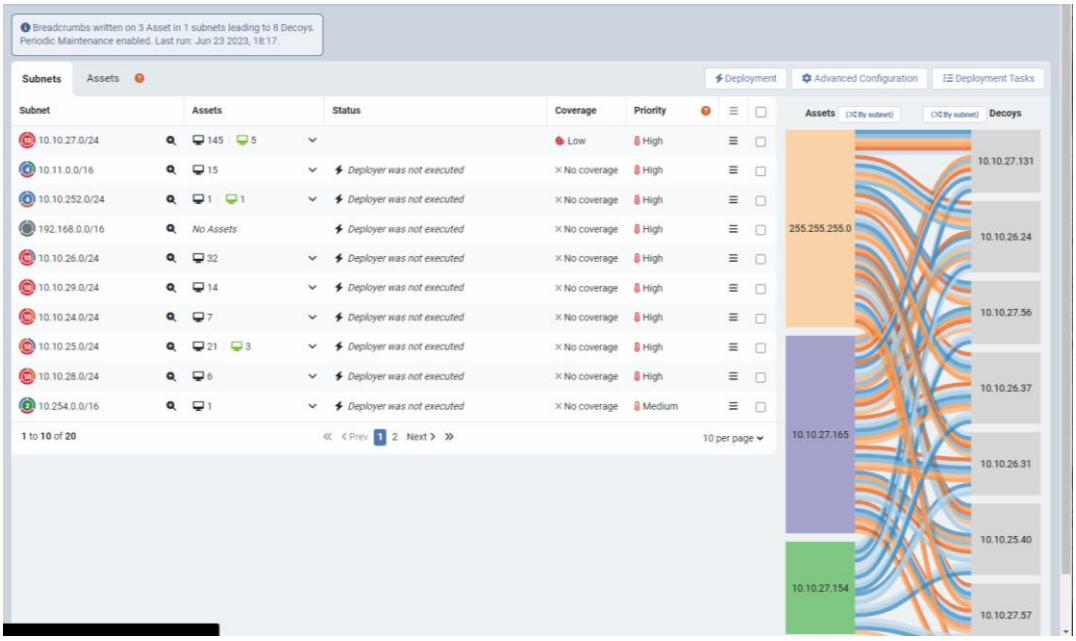

Рис.3.39. Пастки та «хлібні крихти» Fidelis.

Також для під час впровадження даного рішення в організацію, було розроблено список правил, які повинні спрацьовувати в автоматизованому режимі та реагувати на дії користувачів, рис.3.40-3.41.

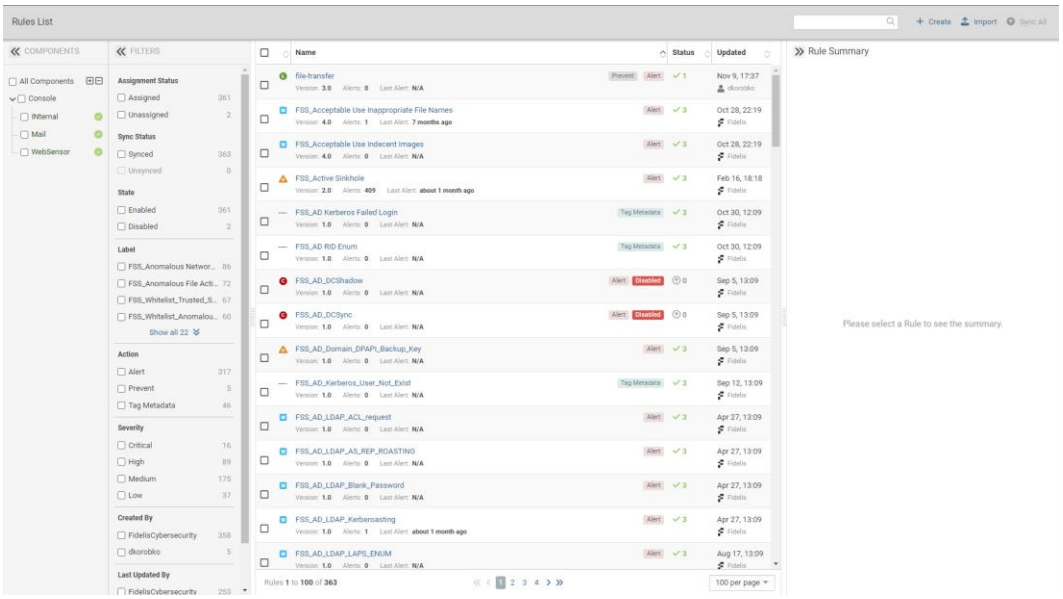

Рис.3.40. Правила Fidelis.

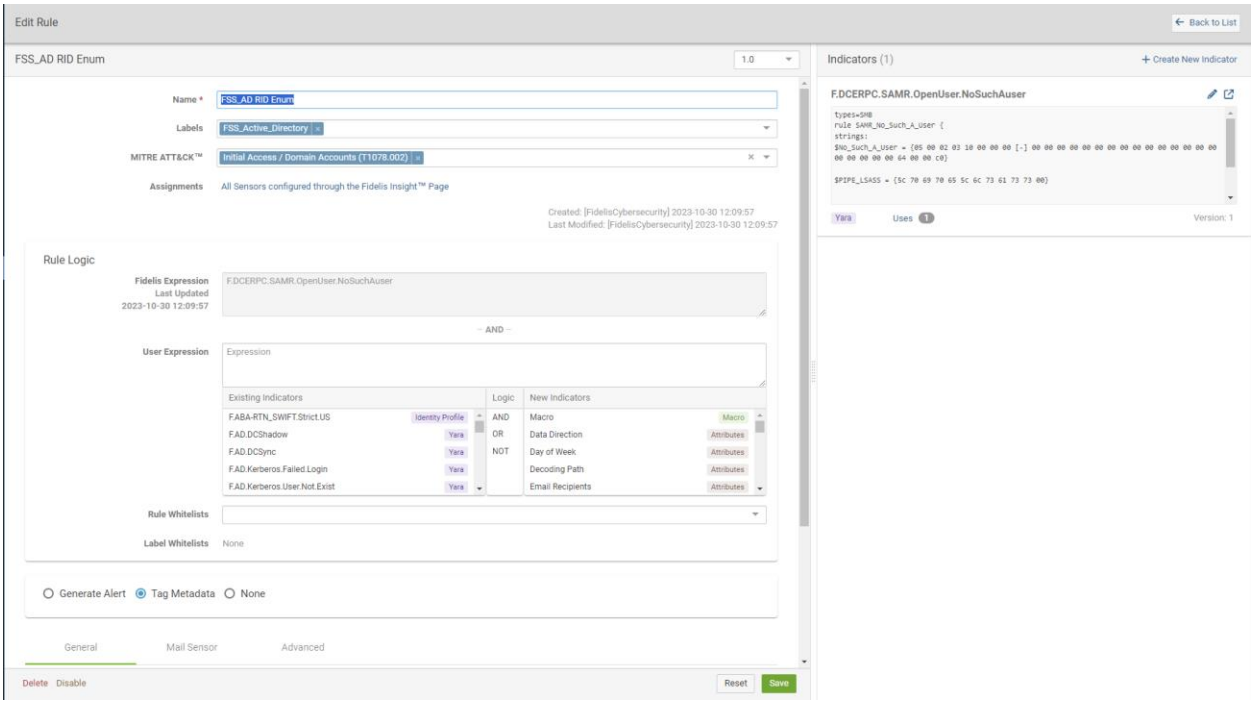

Рис.3.41. Створення правил Fidelis.

3.6. Робота з модулем EndPoint Fidelis

Даний модуль EndPoint, є окремим рішенням з власним способом розгортання. Призначений для маніторингу на кінцевих робочих станціях. На робочу станцію інсталюється за допомогою агенту (спеціальне програмне забезпечення, яке здійснює комунікацію з центром управління Fidelis). За допомогою даного модуля можна здійснювати управління на основі правил, які розробляються та були розроблені в даній роботі на спрацювання певних дій з боку користувачів. На рис.3.42, можна побачити список правил за допомогою, яких здійснюється управління.

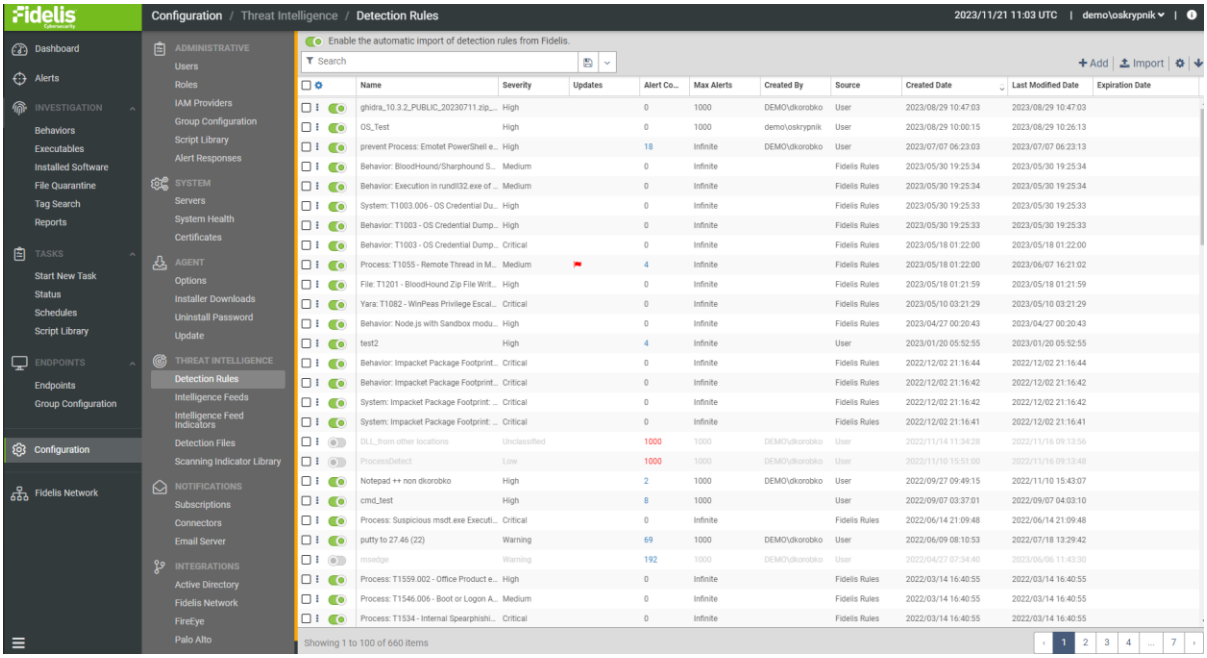

Рис.3.42. Правила Fidelis EndPoint.

За допомогою агенту, який встановлений на робочих станціях, є змога здійснювати повний контроль за робочою станцією користувача. Можна передивлятися спрацювання на станції, наявність вразливостей на ній. Безпосередньо також аналізувати сторонні пристрої, які підключаються до станції. Та за потреби можна підключатися та виконувати команди віддалено на робочих станціях за допомогою CLI-консолі.

На рис.3.43-3.45, можна ознайомитися зі взаємодією з робочими станціями.

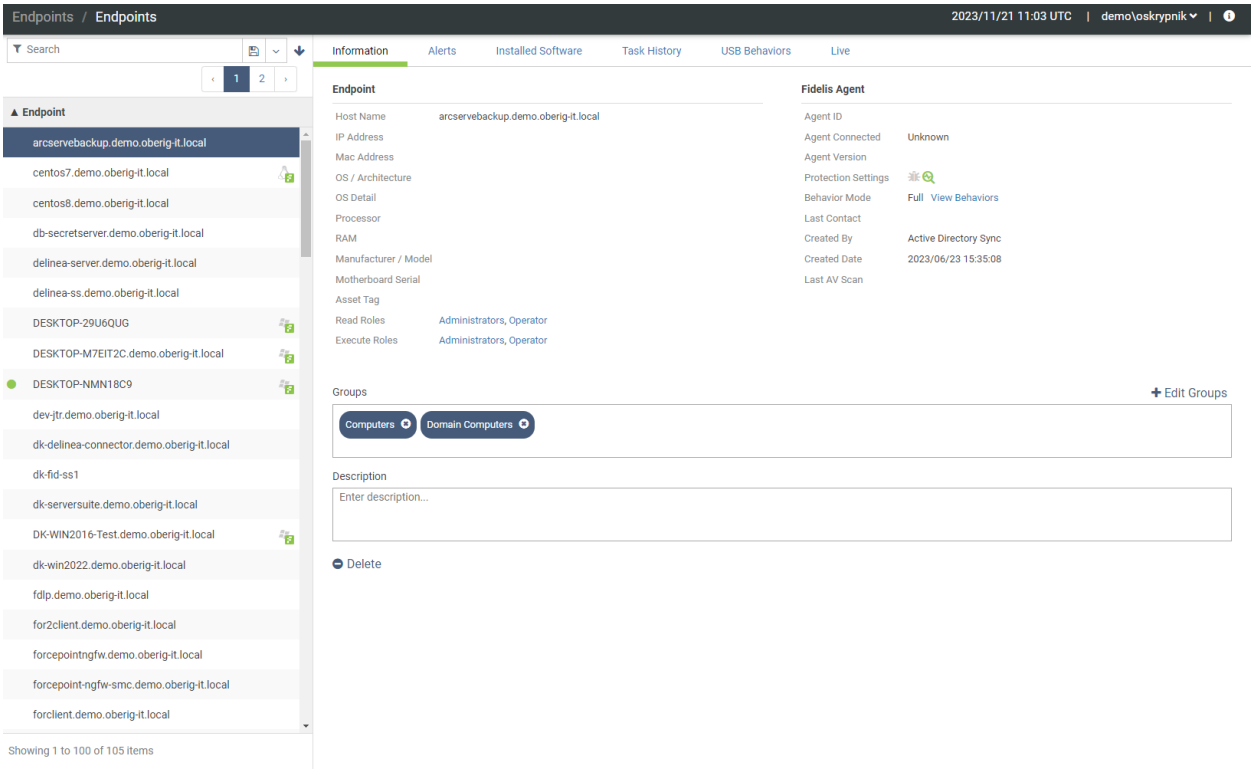

Рис.3.43. Інформація про робочу станцію на якій встановлено агент Fidelis EndPoint.

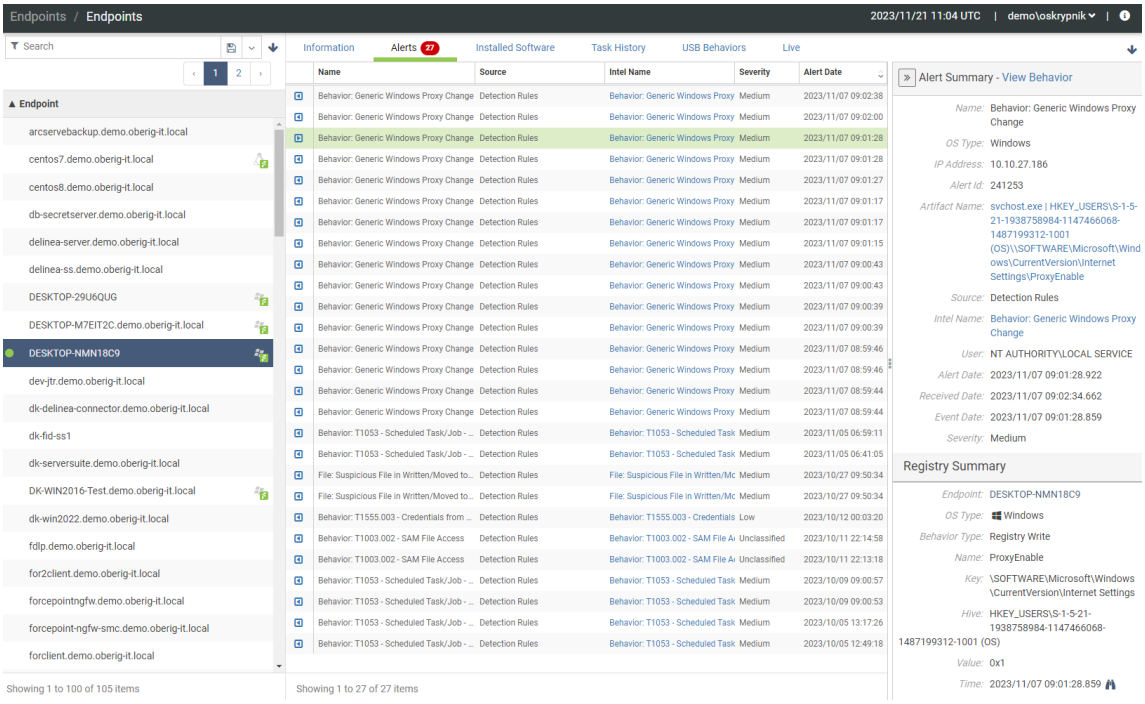

Рис.3.44. Спрацювання на робочій станції Fidelis EndPoint.

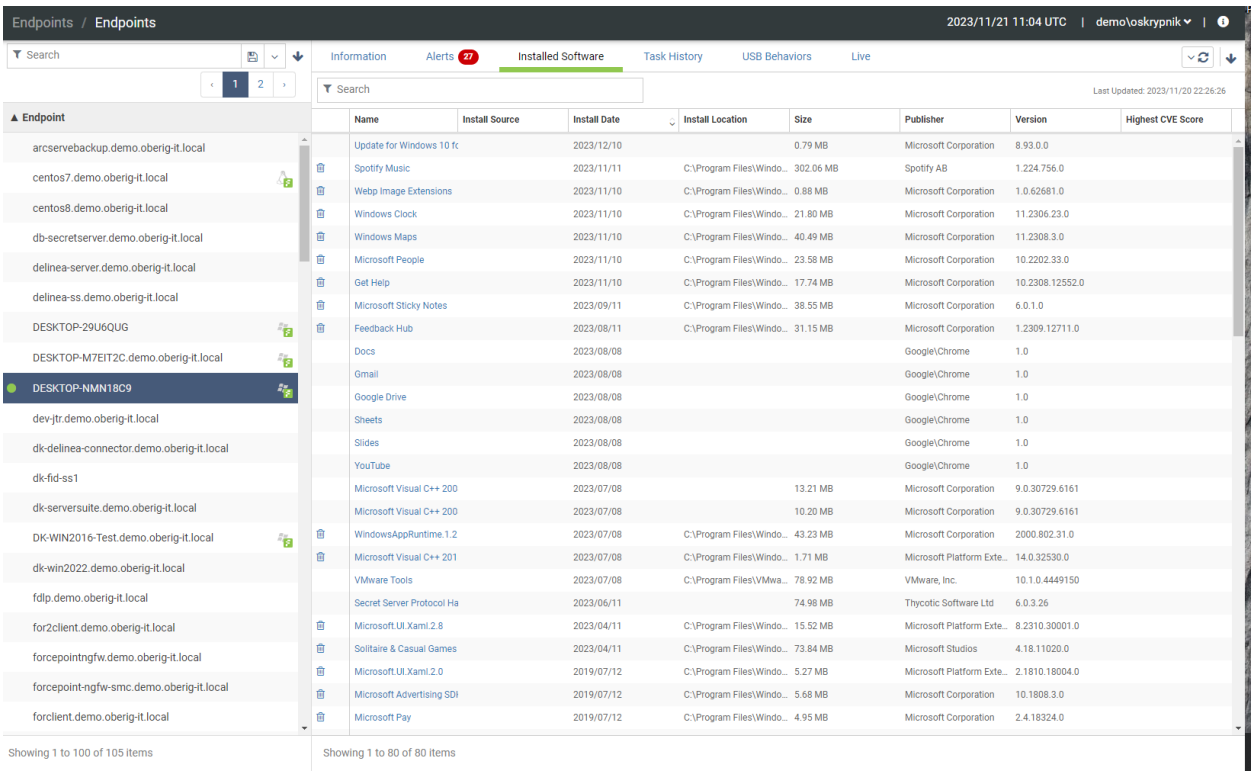

Рис.3.45. Інстальоване програмне забезпечення на робочій станції Fidelis EndPoint.

Під час виконання роботи, було здійснено розробку та інтеграцію програмних комплексів в середовище компанії. Після того, як ці дії були виконані можна бачити, що всі задачі були виконані за допомогою системи PAM, маємо повний контроль над привілейованими користувачами та знижується документообіг, що надало підприємству автоматизацію. На додаток зменшилися витрати на оплату роботи підрядників, тому що виконується запис сесії та активності користувачів.

Система WSS, яка була впроваджена в організації дала змогу автоматизувати дії для блокування веб-ресурсів за допомогою категоризації, а не окремо створюючи White та Black листи. Додатково дане рішення має вбудований антивірус, що дає змогу аналізувати завантажені користувачами файли.

Рішення EDR, дало змогу захистити середовище за допомогою розкидання пасток, що імітують цільові легітимні системи. Додатково здійснюється повний контроль над кінцевими робочими станціями та змога віддалено до них підключатися.

Додатково було розроблено скрипт для Fudo PAM, який доповнив функціональні можливості системи в частині автоматичної ротації парою для WinRM. Лістинг скрипту представлено в додатку Б. Оскільки всі системи можуть здійснювати кастомізацію для Symantec WSS, додатково розроблено код, який дає змогу змінити закладену в систему сторінку блокування відповідно до політики безпеки.

В рішенні Fidelis EDR, розроблено код, який блокує можливість здійснювати видалення користувачем агенту, без відома адміністратора. Таким чином було попереджено можливість обходу детекцію системою дій користувачів.

3.7. Висновки до розділу 3

В даному розділі, було розроблено системи моніторингу та боротьби з кіберзагрозами на базі WSS, EDR та PAM рішень для компанії ОБЕРІГ-ІТ. Зокрема, розроблено базу даних, YARA правила, автоматизовані скрипти, система PAM з роботою правил та детекцію дій користувачів.

Продемонстровано налаштування сучасних інструментів, які забезпечують захист, як внутрішнього периметру організації, так і зовнішнього. Ршення є досить гнучкими до розгортання та масштабування, для забезпечення відмовостійкості.

Показано, що в базовому вигляді рішення недостатньо готове до використання. Тому що потрібно враховувати фактори сьогоднішніх атак, та зловживань прав наданих користувачам на цільових кінцевих точках, які можуть бути використані проти організації. Додатково розроблено правила, на основі яких буде відбуватися спрацювання на дії користувачів. Також додано додатковий функціонал за допомогою кастомних скриптів.

ВИСНОВКИ

В наш час, коли цифровізація торкнулася кожної галузі, потрібно чітко розуміти вектор нових атак та можливість протидіяти їм за допомогою сучасних інструментів. В роботі було розглянуто сучасні види атак та методи протидії, які використовуються в даний момент.

Основною проблемою з якою стикаються організації в розрізі кіберзахисту, це визначення вразливих місць системи та передбачення можливих атаки, які можуть виникнути на внутрішньому периметрі організації.

Внутрішні атаки можуть бути знешкоджені за допомогою PAM рішень, які представлені в роботі. Запропонований у роботі підхід дозволяє повністю контролювати дії користувачів та реагувати на них в реальному часі за допомогою механізму запису відео та аналізу команд, введених користувачами. Такий підхід дозволяє уникнути розголошення авторизаційних даних локальним користувачам, наприклад, підрядникам. Достатньо завести користувача в PAM та надати лише данні для автентифікації на PAM. Крім того, за рахунок автоматизації цих процесів, зменшується обсяг документообігу в організації.

В роботі запропоновано рішення на основі WSS та EDR, які захищають зовнішній периметр, для недопущення зловмисників на внутрішній периметр і забезпечення цілісності інфраструктури компанії.

Для організації «Оберіг ІТ» на основі проведення аналітичного аудиту безпеки, виявлено вразливості і запропоновано рішення на основі систем системи Symantec WSS, Fidelis EDR, XDR та Fudo PAM.

Особливістю організації «Оберіг ІТ» є використання послуг підрядних компаній, що потребує чіткого логування дій підрядників, для виявлення порушень з їх боку та розуміння використаних робочих годин. Розроблена система містить рольову модель за допомогою, якої можна розмежовувати дії адміністраторів, з метою обмеження доступу до певних ресурсів.

Для вирішення задачі контролю виходу користувачів в мережу Інтернет та обмеження їх дій назовні використано підхід WSS, PAM та EDR.

Для здійснення моніторингу мережевої інфраструктури компанії «Оберіг IT» було розгорнуто агентів, які дають можливість спостереження за активним мережевим обладнанням, з подальшим реагуванням та дистанційним адмініструванням.

Додатково було розроблено скрипт для Fudo PAM, який доповнив функціональні можливості системи в частині автоматичної ротації парою для WinRM. Лістинг скрипту представлено в додатку Б. Оскільки всі системи можуть здійснювати кастомізацію для Symantec WSS, додатково розроблено код, який дає змогу змінити закладену в систему сторінку блокування відповідно до політики безпеки.

В рішенні Fidelis EDR, розроблено код, який блокує можливість здійснювати видалення користувачем агенту, без відома адміністратора. Таким чином було попереджено можливість обходу детекцію системою дій користувачів.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ ВИКОРИСТАНИХ ДЖЕРЕЛ

1. IATF 16949 [Електронний ресурс] Режим доступу: https://ru.wikipedia.org/wiki/IATF_16949 (дата звернення 10.07.23) – Назва екрана.

2. Gobuster [Електронний ресурс] Режим доступу: https://github.com/OJ/gobuster (дата звернення 10.07.23) – Назва екрана.

3. Огляд Fudo PAM. [Електронний ресурс] Режим доступу: https://fudosecurity.com/ (дата звернення 11.07.23) - Назва екрана.

4. Функціональні можливості Fudo PAM [Електронний ресурс] Режим доступу: https://fudosecurity.com/ (дата звернення 11.07.23) - Назва екрана.

5. Методи підключення до Fudo PAM [Електронний ресурс] Режим доступу: https://download.fudosecurity.com/documentation/fudo/5_3/online/ (дата звернення 11.07.23) - Назва екрана.

6. Огляд Fidelis Deception [Електронний ресурс] https://fidelissecurity.com/fidelis-elevate/ Режим доступу: (дата звернення 15.08.23) - Назва екрана.

7. Опис Symantec [Електронний ресурс] Режим доступу: https://techdocs.broadcom.com/us/en/symantec-security-software.html (дата звернення 20.09.23) - Назва екрана.

8. Опис Symantec [Електронний ресурс] Режим доступу: https://techdocs.broadcom.com/us/en/symantec-security-software.html (дата звернення 20.09.23) - Назва екрана.

9. SQL опис [Електронний ресурс] Режим доступу: https://ru.wikipedia.org/wiki/SQL (дата звернення 25.10.23) - Назва екрана.

10. Початок налаштування Fudo PAM [Електронний ресурс] Режим доступу: https://download.fudosecurity.com/documentation/fudo/5_3/online (дата звернення 07.04.22) – Назва екрана.

ДОДАТКИ

Додаток А

Програмна реалізація кастомної сторінки сповіщення блокування політикою WSS Symantec

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8">
    <title>Access Denied</title>
    <style>
      body {
        margin: 0;
        padding: 0;
        font-family: Arial, sans-serif;
        background-color: #f2f2f2;
      }
      .container {
        max-width: 600px;
        margin: 0 auto;
        text-align: center;
        padding-top: 50px;
      }
      .error-code {
        font-size: 72px;
        font-weight: bold;
        color: #e74c3c;
        margin-bottom: 0;
```

```
}
    h1 {
      font-size: 32px;
      color: #e74c3c;
      margin-top: 20px;
    }
    p {
      font-size: 20px;
      color: #444444;
      margin-top: 10px;
    }
    .cta-button {
      display: inline-block;
      margin-top: 20px;
      padding: 10px 20px;
      background-color: #e74c3c;
      color: #ffffff;
      text-decoration: none;
      border-radius: 5px;
      transition: background-color 0.3s;
    }
    .cta-button:hover {
      background-color: #c0392b;
    }
  </style>
</head>
```

```
<body>
 <img src= https://scontent-iev1-1.xx.fbcdn.net/v/t39.30808-6/275500663_1641943116156836_1134236537787219856_n.png?stp=dst-png_p600x600&_nc_cat=102&ccb=1-7&_nc_sid=e3f864&_nc_ohc=U9kAT1Uk2pQAX-n_jI3&_nc_ht=scontent-iev1-1.xx&oh=00_AfA3lmhdblJhb-N0NUwU9ynHcfhYwL2MkYk5d0kdfjJp8Q&oe=64273787 alt= "logo company" style="width:1000px; height:400px;">
  <div class="container">
   <h1>Access Denied</h1>
   <p>We're sorry, but your request to access this website has been denied due to company policy.</p>
   <p>Please contact your IT department if you believe this is an error.</p>
   <a href="#" class="cta-button">Go Back</a>
  </div>
 </body>
</html>
```

Програмна реалізація зміни паролю для WinRM Fudo PAM


```
{ "name": "test_changer_00567",
"timeout": 300,
"transport": "WinRM",
"changer_type": "change",
"variables": [
    {
        "id": "7394910588142354434",
        "name": "transport_bind_ip",
        "description": null,
        "encrypt": false,
        "required": false,
        "object_type": "fudo_server",
        "object_property": "bind_ip"
    },
    {
        "id": "7394910588142354435",
        "name": "transport_ca_certificate",
        "description": null,
        "encrypt": false,
        "required": false,
        "object_type": "fudo_server",
        "object_property": "transport_ca_certificate"
    },
    {
        "id": "7394910588142354436",
        "name": "transport_encoding",
        "description": null,
        "encrypt": false,
        "required": false,
        "object_type": null,
        "object_property": null
    },
    {
        "id": "7394910588142354437",
        "name": "transport_host",
        "description": null,
        "encrypt": false,
        "required": false,
        "object_type": "fudo_server",
        "object_property": "address"
    },
    {
        "id": "7394910588142354438",
        "name": "transport_login",
        "description": null,
        "encrypt": false,
        "required": false,
        "object_type": "fudo_account",
        "object_property": "login"
    },
    {
        "id": "7394910588142354439",
        "name": "transport_port",
        "description": null,
        "encrypt": false,
```

"required": false,


```
        "object_type": "fudo_server",
        "object_property": "port"
    },
    {
        "id": "7394910588142354440",
        "name": "transport_secret",
        "description": null,
        "encrypt": false,
        "required": false,
        "object_type": "fudo_account",
        "object_property": "secret"
    },
    {
        "id": "7394910588142354441",
        "name": "x",
        "description": null,
        "encrypt": false,
        "required": false,
        "object_type": null,
        "object_property": null
    }
],
"commands": [
    {
        "id": "7394910588142354434",
        "command": "echo %%x%%",
        "expected": null,
        "delay": null,
        "comment": null,
        "position": 0
    }]}
```

Програмна для блокування видалення агенту Fidelis

```
#!/bin/bash

#Remove agent
sleep 5
rm -rf /usr/FidelisTemp
logfile=/tmp/fidelis_endpoint.log
INITD=/etc/init.d/endpoint
INITDCHANGED="no"
INITDORIG=/etc/init.d/endpoint
PROTECTINITD=/etc/init.d/protect
PROTECTCONFENABLED=/etc/init/protect.conf
if [ `ps --pid 1 -o cmd | grep systemd | wc -l` == 1 ] && [ -e /usr/lib/systemd/system ]; then
        INITD=/usr/lib/systemd/system/endpoint.service
        PROTECTINITD=/usr/lib/systemd/system/protect.service

elif [ `command -v systemctl | wc -l` == 1 ] && [ -e /lib/systemd/system ]; then
        INITD=/lib/systemd/system/endpoint.service
        PROTECTINITD=/lib/systemd/system/protect.service
        INITDCHANGED="yes"

elif [ `command -v initctl | wc -l` == 1 ]; then
        INITD=/etc/init/endpoint.conf
        PROTECTINITD=/etc/init/protect.conf.disabled
        INITDCHANGED="yes"
fi


        if [ -d "$1/drivers" ]; then
          #redhat7
          if [[ $INITD =~ .*service ]]; then
                systemctl disable protect.service > /dev/null 2>&1
                systemctl stop protect.service > /dev/null 2>&1
          #ubuntu 14 | redhat 6
          elif [[ $INITD =~ .*conf ]]; then
                initctl stop protect > /dev/null 2>&1
          #suse | redhat
          fi

          rm -rf $PROTECTINITD > /dev/null 2>&1
          if [[ $INITD =~ .*conf ]]; then
                rm -rf $PROTECTCONFENABLED > /dev/null 2>&1
          fi
```

Продовження додаток В

```
  #stop the driver
  "$1/drivers/bin/uninstall.sh"
  rm $PROTECTINITD
 fi

 rm -rf "$installPath/../../../Fidelis" > /dev/null 2>&1
 rm -rf "/usr/Fidelis" > /dev/null 2>&1

 #Shutdown the agent after shutting down protect
 #redhat7
 if [[ $INITD =~ .*service ]]; then
  systemctl disable endpoint.service > /dev/null 2>&1
  rm -rf $INITD
  #systemctl stop endpoint.service > /dev/null 2>&1

 #ubuntu 14 | redhat 6
 elif [[ $INITD =~ .*conf ]]; then
  rm -rf $INITD
  #initctl stop endpoint > /dev/null 2>&1
 #suse | redhat
 else
  /sbin/chkconfig --del endpoint >> $logfile 2>&1
  if [ `grep "fe:345:respawn:/etc/init.d/endpoint try-start" /etc/inittab | wc -l` == 1 ]; then
        echo "$(grep -v "fe:345:respawn:/etc/init.d/endpoint try-start" /etc/inittab)" >
/etc/inittab
  fi
 fi

 rm -rf $INITD > /dev/null 2>&1

 if [[ $INITD =~ .*service ]]; then
  systemctl daemon-reload
  systemctl reset-failed
 elif [[ $INITD =~ .*conf ]]; then
  initctl reload-configuration > /dev/null 2>&1
 fi
 kill -TERM $(ps aux | grep -v grep | grep Platform/endpoint | awk '{print $2}')
```