ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ВИЯВЛЕННЯ ВТОРГНЕНЬ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ НА БАЗІ DECEPTION-ТЕХНОЛОГІЇ»

Виконав студент 6 курсу, групи БСДМ-62
спеціальності 125 Кібербезпека освітньо-професійної програми«Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Калиндрузь Б.М.
(прізвище та ініціали)
Керівник Гайдур Г.І.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2022

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
“___”_____ 2021 року

ЗАВДАННЯ
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Калиндрузю Богдану Миколайовичу
(прізвище, ім’я, по батькові)

1. Тема магістерської роботи: «Виявлення вторгнень до Інформаційної системи організації на базі Deception-технології»

керівник магістерської роботи Гайдур Галина Іванівна д.т.н., доцент,
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «___» _____ 2021 року №____.

2. Строк подання студентом магістерської роботи 15.12.2021 р.

3. Вихідні дані до магістерської роботи корпоративна інформаційна система; наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Актуальність проблеми виявлення вторгнень до Інформаційних систем організацій.
2. Методи та засоби виявлення вторгнень.
3. Порядок застосування deception-технології для виявлення вторгнень до інформаційної системи організації.

5. Перелік графічного матеріалу
1. Тема магістерської роботи.
2. Об’єкт, предмет, мета та наукові завдання дослідження.
3. Результати аналізу проблем захисту ІС компаній.
4. Результати аналізу методів та засобів виявлення вторгнень до ІС компаній.
5. Рекомендації щодо застосування технології Deception для виявлення вторгнень до ІС компанії.
6. Висновки за результатами роботи.

6. Дата видачі завдання 27.09.2021 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів роботи	Примітка
1.	Уточнення постановки завдання	14.10.2021	
2.	Аналіз технічної літератури	20.10.2021	
3.	Аналіз методів виявлення вторгнень	25.10.2021	
4.	Розробка порядку застосування deception-технології для виявлення вторгнень до інформаційної системи організації	15.11.2021	
5.	Оформлення результатів дослідження. Проходження плагіату	15.12.2021	
6.	Підготовка доповіді до захисту.	19.12.2021	

Студент Калиндрузь Б.М.
(підпис) прізвище та ініціали

Керівник магістерської роботи Гайдур Г.І.
(підпис) прізвище та ініціали

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ МАГІСТЕРСЬКОЇ РОБОТИ

Направляється студент Калиндрузь Б.М. до захисту магістерської роботи
(прізвище та ініціали)
спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Технологія управління захистомкінцевих точок корпоративної інформаційної системи на базі ESET Security Management Center».

Магістерська робота і рецензія додаються.

Директор інституту _____ Савченко В.А.
(підпис) (прізвище та ініціали)

Довідка про успішність

Калиндрузь Б.М. за період навчання в інституті
(прізвище та ініціали студента)
ННІЗІ з 2020 року по 2022 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.

Секретар інституту _____ Журенко О.В.
(підпис) (прізвище та ініціали)

Висновок керівника магістерської роботи

Студент ***Калиндрузь Б.М.***, обрав тему роботи, метою якої було дослідити зміст технології Deception, а саме виявлення вторгнень до інформаційної системи компанії та розробити порядок її застосування на підприємстві. Перелік використаних джерел свідчить про вміння магістром розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання магістерської роботи Калиндрузь Б.М. показав відмінну теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану магістерську роботу студента Калиндрузя Богдана Миколайовича на оцінку **«відмінно»** та присвоїти йому кваліфікацію магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Керівник магістерської роботи Гайдур Г.І.
(підпис) (прізвище та ініціали)
“____” _____ 2021 року

Висновок кафедри про магістерську роботу

Магістерська робота розглянута. Студент Калиндрузь Б.М.
(прізвище та ініціали)
допускається до захисту даної магістерської роботи в Державній екзаменаційній комісії
Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

Гайдур Г.І.
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Текстова частина магістерської кваліфікаційної роботи: 81 стор., 36 рис., 1 табл., 19 джерел.

Мета роботи – дослідження принципів і методів виявлення вторгнень до інформаційних систем.

Об'єкт дослідження – процес виявлення вторгнень до інформаційних систем.

Предмет дослідження – створення пасток на основі Deception-технології.

Короткий зміст роботи: В роботі приведено основні відомості про системи виявлення вторгнень до інформаційних систем на основі Deception-технології. Висвітлено проблеми захисту ІС компаній. Проведено аналіз методів та засобів виявлення вторгнень до інформаційної системи організації та розроблено порядок застосування технології.

.

DECEPTION TECHNOLOGY, HONEYPOT, HONEYNET, DECEPTION, ЗАХИСТ ІНФОРМАЦІЙНИХ СИСТЕМ

ABSTRACT

Text part of the master's qualification work: 81 pages, 36 pictures, 1 table, 19 sources.

The purpose of the work is to study the principles and methods of detecting intrusions into information systems.

Object of research - The process of detecting intrusions into information systems.

Subject of research - Creating traps based on Deception-technology.

Summary of the work: The paper provides basic information about intrusion detection systems for information systems based on Deception-technology. Problems of IP protection of companies are highlighted. The analysis of methods and means of detection of intrusions into the information system of the organization is carried out and the order of application of technology is developed.

.

DECEPTION TECHNOLOGY, HONEYPOT, HONEYNET, DECEPTION, PROTECTION OF INFORMATION SYSTEMS

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

СВВ - Системи виявлення вторгнень

ІС – Інформаційна система

ШІ - Штучний інтелект

ВСТУП

Інтернет – це нове поле битви 21 століття, коли інформаційна війна стає настільки ж поширеною, руйнівною та потенційно смертельною, як і більш традиційні форми війни.

Незважаючи на загалом більшу обізнаність про кіберзагрози та увагу до IT-безпеки, кількість та масштаби успішних кібератак продовжують зростати з тривожними темпами. Навряд чи обходиться місяць без новин про масовий злом даних, який зачіпає мільйони жертв, і багато підприємств уже були скомпрометовані — вони просто ще не знають про це. У звіті Verizon Data Breach Investigations Report за 2021 рік виявлено, що майже 50 відсотків загроз залишаються непоміченими в мережах підприємства-жертви — таємно вилучаючи цінні інформаційні активи (наприклад, конфіденційну інформацію про клієнтів, дані кредитних карток та інтелектуальну власність) — протягом днів, тижнів або місяців.

Еволюція часто покладалася на обман як на техніку виживання. Для істот з вищими когнітивними здібностями здатність обманювати пов’язана з творчістю. Для успішної брехні використовуються ті самі когнітивні навички, які дозволяють уявити. Винахідливість людства ще більше вдосконалила задум природи і перетворила обман на мистецтво. Цитуючи римського філософа Цицерона, «Мистецтво народжується із спостереження й дослідження природи».

Отже, що ми можемо дізнатися про обман від природи:

- Різноманітні: є буквально тисячі прикладів обману.
- Спеціалізовані: кожен тип обману працює лише для певного виду, у певному середовищі, для конкретної загрози чи можливостей.
- Динамічний: гонка озброєнь між хижаком і жертвою продовжує генерувати нові обмани, оскільки супротивники розвиваються, щоб обійти попередні обмани.

Обман завжди був стратегічним компонентом війни. У «Мистецтві війни» Сунь Цзи обман є ключовим принципом ведення війни. Протягом усієї історії використовувалися різні прийоми, щоб залучити супротивника в слабку позицію, або щоб перемогти або повністю розгромити ворога.

Протягом історії війни використовувалися різні типи обманних тактик, наприклад:

- Удаваний відхід: ведення ворога через хибне відчуття безпеки в попередньо встановлену засідку. У стародавні часи Ганнібал використовував цю тактику, щоб створити враження, що центр його ліній відходить, а потім згорнув свої фланги до римської армії, коли вона просувалася до оманливо слабкого центру.
- Вигадані підрозділи: створення повністю вигаданих сил або перебільшення розміру армії. У битві при Мегіддо під час Першої світової війни союзні війська використали 15 000 бутафорських коней (або коней для манекенів?), щоб обдурити османів і перешкодити їм відійти до узбережжя.
- Димова завіса: використання диму, туману чи інших затемнення, щоб приховати рух на полі бою. Протягом усієї історії димові завіси використовувалися у сухопутній та морській війні.
- Стратегічне охоплення: розгортання невеликих сил, щоб відволікти противника, тоді як набагато більші сили рухаються для атаки з тилу. Це була улюблена тактика Наполеона Бонапарта.
- Троянський кінь: отримання доступу до укріпленого району під фальшивими приводами, щоб згодом прийняти більші атакуючі сили. Найвідомішим прикладом є хитрість, яку використовували греки, щоб увійти в Трою. Як і в природі, є кілька важливих уроків про обман, які ми можемо винести з війни. Успішний обман у війні завжди є результатом надзвичайно добре організованого та добре виконаного плану і залежить від наступного:
- Секретність: обман повинен зливатися з навколишнім середовищем. Коли в битві при Мегіддо використовували фіктивних коней, справжніх коней вигулювали до найближчого джерела води кілька разів на день, щоб доповнити ілюзію.

- Оригінальність: один і той же обман не можна використовувати кілька разів, і він не підходить за будь-яких обставин.

Оскільки сучасне поле битви поширилося на кіберпростір, також з’явилася тактика ведення війни, включаючи обман. Обман був використаний в одному з найперших відомих і найвідоміших випадків злому телефонів, або «фрікінг». У 1971 році Джон Дрейпер використав іграшковий свисток із коробки зернових Cap'n Crunch, щоб імітувати тон 2600 герц (Гц) довгих ліній AT&T, які вказували, коли магістральна лінія була готова та доступна. щоб перенаправити новий виклик. Цей обман дозволив хакерам здійснювати безкоштовні міжміські дзвінки.[1]

Gartner прогнозує, що до 2022 року 25% усіх проектів виявлення загроз та реагування на них будуть включати функції обману та функціональні можливості.[2]

1. АНАЛІЗ ВИЯВЛЕННЯ ВТОРГНЕНЬ

1.1 Методи виявлення вторнгень

Виявлення порушення безпеки проводиться зазвичай з використанням евристичних правил і аналізу сигнатур відомих комп'ютерних атак. Вже в 1984 році Фред Коен заявив, що кожне вторгнення виявити неможливо і ресурси, необхідні для виявлення вторгнень, будуть рости разом зі ступенем використання комп'ютерних технологій [3].

Найбільш поширеними є, так звані локальні і мережеві «Системи виявлення вторгнень». Локальна СВВ передбачає, що система виявлення встановлюється на кожному окремому комп'ютері. Мережева СВВ збирає пакети, що надходять в мережу через один пристрій і аналізує їх, перш ніж пересилати заданим вузлам. Мережеві СВВ сьогодні вважаються менш ефективними, адже чим більша кількість вузлів в мережі тим важче стає забезпечення надійної фільтрації пакетів і, як наслідок, захист комп'ютерів в мережі.

Системи виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак на інформаційні системи вже давно застосовуються як один з необхідних рубежів оборони інформаційних систем і використовуються для виявлення деяких типів шкідливої активності, яка може негативно вплинути на безпеку комп'ютерної системи. До такої активності відносяться мережеві атаки, що спрямовані проти вразливих сервісів, атаки, які передбачають підвищення привілеїв, неавторизований доступ до важливих файлів, а також дії шкідливого програмного забезпечення (комп'ютерних вірусів, троянів і черв'яків).

4 листопада 1983 був винайдений перший комп'ютерний вірус [3]. Фред Коен у той час ще аспірант одного з американських університетів, написав першу програму-вірус, яка здатна до саморозмноження та паразитичного поширення по мережах. На презентації своєї докторської дисертації, яка була присвячена проблемі забезпечення безпеки комп'ютерних систем Коен представив першу програму-вірус. Особливої загрози програма Коена не становила, оскільки експеримент був контрольованим і не мав далекосяжних цілей.

На сьогоднішній день виділяють і рекомендують до застосування, в тому числі, і при побудові системи захисту три групи методів виявлення атак:

- сигнатурні методи;
- методи виявлення аномалій;
- комбіновані методи (використовують спільно алгоритми, визначені в сигнатурних методах і методах виявлення аномалій).

Іншими словами, виявлення порушення безпеки проводиться зазвичай з використанням евристичних правил і аналізу сигнатур відомих комп'ютерних атак.

1.1.1 Сигнатурні методи

Сигнатурні методи описують кожну атаку особливою моделлю або сигнатурою, в якості якої можуть застосовуватися рядок символів семантичний вираз на спеціальній мові, використанням спеціалізованої бази даних формальна математична модель і т. д. Сутність сигнатурного методу в наступному: у вихідних даних, зібраних мережевими і хостовими датчиками системи виявлення вторгнення з сигнатур атак, виконується процедура пошуку сигнатури атаки. Перевага даних методів висока точність визначення факту атаки, а очевидним недоліком є неможливість виявлення атак, сигнатури яких ще не визначені [4].

Серед сигнатурних методів виявлення атак найбільш поширений метод контекстного пошуку, який полягає в виявленні у вихідній інформації певної безлічі символів. Так, для виявлення атаки на Web-сервер, що спрямована на отримання несанкціонованого доступу до файлу паролів, проводиться пошук послідовності символів "GET * / etc / passwd" у заголовку HTTP-запиту. Фрагмент "cwd ~root" в FTP-сеанс однозначно визначає факт обходу механізму аутентифікації на FTP-сервері і спробі перейти в кореневий каталог FTP-сервера. Іншим прикладом є виявлення аплетів Java в мережевому трафіку на основі шістнадцятирічного фрагмента "CA FE BA BE". Ці ж сигнатури дозволяють виявляти троянських коней, якщо останні використовують

стандартні значення портів. Наприклад, троян NetBus, визначається по використанню 12345-го і 12346го портів, а троян BackOrifice 31337-го порту [3].

Для розширення функціональних можливостей контекстного пошуку в деяких випадках використовуються спеціалізовані мови, що описують сигнатуру атаки. На рисунку 1.1 наведено приклад сигнатури атаки Land, описаної за допомогою мови N-code системи NFR.

```
filter pptp ip ()
{
# Если IP-адрес отправителя пакета # данных Совпадает с IP-
адресом
# получателя, то в журнал записывается # информация об атаке
Land
   if (ip.src == ip.dest)
   {
      system.time, eth.src, ip.src, sth.dst to land_recrdr;
   }
}
```

Рисунок 1.1. Приклад сигнатури атаки Land

За допомогою контекстного пошуку ефективно виявляються атаки на основі аналізу мережевого трафіку, оскільки даний метод дозволяє найбільш точно задати параметри сигнатури, яку необхідно виявити в потоці вихідних даних.

У ряді академічних СВВ були реалізовані ще два сигнатурних методи: метод аналізу станів і метод, який базується на експертних системах. Метод аналізу станів або контролю частоти подій заснований на формуванні сигнатури атак у вигляді послідовності переходів інформаційної системи ІС з одного стану в інший. По суті, кожен такий перехід визначається по настанню в ІС певної події, а набір цих подій задається параметрами сигнатури атаки. Ці сигнатури описують ситуації, коли протягом деякого інтервалу часу відбуваються події, число яких перевищує задані заздалегідь показники. Прикладом такої сигнатури є виявлення сканування портів або виявлення

атаки SYN Flood. У першому випадку пороговим значенням є число портів, перевірених в одиницю часу. У другому випадку число спроб встановлення віртуального з'єднання з вузлом за одиницю часу [3].

Як правило, сигнатури атак, створені на основі аналізу станів, описуються математичними моделями, що базуються на теорії кінцевих автоматів або мереж Петрі.

На рисугку 1.2 показана мережа Петрі, що описує сигнатуру атаки, яка виконує підбір пароля для отримання несанкціонованого доступу до ресурсів ІС. Кожен перехід ІС в новий стан в цій мережі Петрі пов'язаний зі спробою введення пароля. Якщо користувач протягом 1 хв чотири рази поспіль введе неправильний пароль, то метод зафіксує факт здійснення атаки[5].

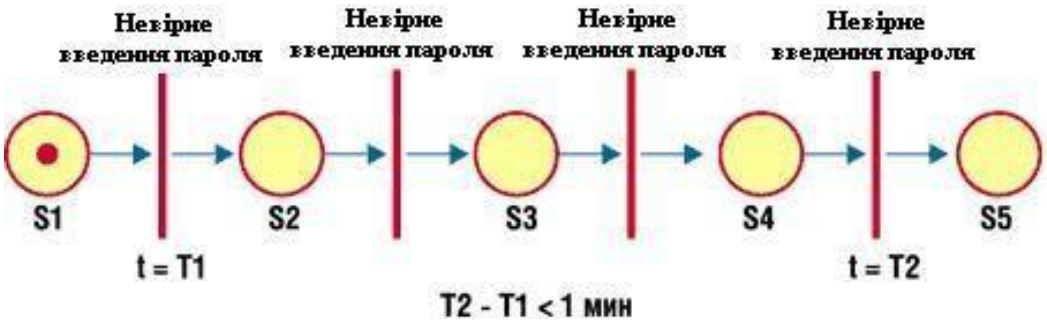

Рис. 1.2. Мережа Петрі, що описує сигнатуру атаки, яка здійснює підбір пароля

Методи, що базуються на експертних системах, дозволяють описувати моделі атак на природній мові з високим рівнем абстракції. Експертна система, яку покладено в основу методів цього типу, складається з двох баз даних: фактів і правил. Факти це вихідні дані про роботу ІС, а правила алгоритми логічних рішень про факт атаки на основі набору фактів. Всі правила експертної системи записуються в форматі "якщо <...>, то <...>". Результуюча база правил повинна описувати характерні ознаки атак, які зобов'язана виявляти СВВ[5].

Одна з найбільш перспективних сигнатурних груп методи, які засновані на біологічних моделях. Для їх опису можуть використовуватися генетичні або нейромережеві алгоритми.

1.1.2 Метод виявлення аномалій або поведінковий метод

Поведінкові методи базуються не на моделях інформаційних атак, а на моделях штатного функціонування (поведінки) ІС. Принцип роботи будь-якого з таких методів полягає в виявленні не відповідності між поточним режимом роботи ІС і режимом роботи, що відповідає штатної моделі даного методу. Будь-яка невідповідність розглядається як інформаційна атака.

Наприклад, якщо система виявлення атак фіксує вхід співробітника компанії в мережу в суботу о 2.30, то це може свідчити про те, що пароль цього користувача вкрадений або підібраний і його зловмисник використовує для несанкціонованого проникнення [3].

Перевага методів даного типу можливість виявлення нових атак без модифікації або поновлення параметрів моделі. На жаль, створити точну модель штатного режиму функціонування ІС дуже складно.

Серед поведінкових методів найбільш поширені ті, що базуються на статистичних моделях. Такі моделі визначають статистичні показники, що характеризують параметри штатної поведінки системи. Якщо з часом спостерігається певне відхилення даних параметрів від заданих значень, то фіксується факт виявлення атаки. Як правило, в якості таких параметрів можуть виступати рівень завантаження процесора, навантаження на канали зв'язку, штатний час роботи користувачів системи, кількість звернень до мережевих ресурсів і т. д.

Слід зазначити, що на стадії рекогносцировки, коли здійснюється збір інформації, ефективні лише сигнатурні методи виявлення атак. Справа в тому, що всі операції отримання необхідної порушнику інформації в більшості випадків не викликають ніякого відхилення роботи ІС від штатного режиму. Для цього етапу характерні такі ознаки, як формування запиту до DNS-сервера, отримання інформації з бази даних SNMP MIB або багаторазові TCPзапити на встановлення з'єднання з різними портами. На стадії рекогносцировки можуть використовуватися як мережеві, так і хостові

датчики [5].

1.1.3 Застосовність сигнатурного і поведінкового методів для виявлення різних стадій атак

На стадії вторгнення виявити атаку можна за допомогою як сигнатурних, так і поведінкових методів. Будь-яке вторгнення характеризується певними ознаками, які, з одного боку, можна представити у атак:

- слабкі можливості по виявленню нових
- на початкових етапах неможливо визначити
- вигляді сигнатури, а з іншого описати як якесь відхилення від штатної поведінки ІС. Найбільш ефективно поєднання обох методів, при цьому для отримання необхідних вихідних даних застосовні будьякі (хостові або мережеві) датчики.

Ефективне виявлення атак на етапах атакуючого впливу і розвитку атаки можливо тільки за допомогою поведінкових методів. Оскільки дії порушників залежать від цілей проведеної атаки і фіксованою безліччю сигнатур атак однозначно не визначаються. З огляду на той факт, що на двох останніх стадіях життєвого циклу інформаційної атаки найхарактерніші об'єкти це хости, в даному випадку найбільш доцільно застосування хостових датчиків.

1.2 Проблеми захисту ІС компаній

Захист інформації є однією з вічних проблем. Протягом історії людства способи розв'язання цієї проблеми визначались рівнем розвитку технологій. У сучасному інформаційному суспільстві технологія відіграє роль активатора цієї проблеми - комп'ютерні злочини стали характерною ознакою сьогодення. Комп'ютерними називають злочини, пов'язані з втручанням у роботу комп'ютера, і злочини, в яких комп'ютери використовуються як необхідні технічні засоби. Серед причин комп'ютерних злочинів і пов'язаних з ними викрадень інформації головними є наступні:

- швидкий перехід від традиційної паперової технології зберігання та передавання інформації до електронної за одночасного відставання технологій захисту інформації, зафіксованої на машинних носіях;
- широке використання локальних обчислювальних мереж, створення глобальних мереж і розширення доступу до інформаційних ресурсів;
- постійне ускладнення програмних засобів, що викликає зменшення їх надійності та збільшення кількості уразливих місць [6].

Сьогодні ніхто не може назвати точну цифру загальних збитків від комп'ютерних злочинів, але експерти погоджуються, що відповідні суми вимірюються мільярдами доларів. Варто також враховувати й моральнопсихологічні наслідки для користувачів, персоналу і власників КС та інформації. Що ж до порушення безпеки так званих «критичних» додатків у державному і військовому управлінні, атомній енергетиці, медицині, ракетно-космічній галузі та у фінансовій сфері, то воно може призвести до тяжких наслідків для навколишнього середовища, економіки і безпеки держави, здоров'я і навіть для життя людей. У сфері захисту інформації та комп'ютерної безпеки в цілому найбільш актуальними є три групи проблем:

- порушення грифу обмеження доступу;
- порушення цілісності інформації;
- порушення дієздатності інформаційно-обчислювальних систем.

Захист інформації перетворюється у найважливішу проблему державної безпеки, коли мова йде про державну, дипломатичну, військову, промислову, медичну, фінансову та іншу таємну інформацію. Величезні масиви такої інформації зберігаються в електронних архівах, оброблюються в інформаційних системах та передаються через телекомунікаційні мережі. Основні властивості цієї інформації – конфіденційність та цілісність, повинні підтримуватись законодавчо, юридично, а також організаційними, технічними та програмними методами. Згідно із Законом України «Про захист інформації в автоматизованих системах» захист інформації - це сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією. У літературі

вживаються також споріднені терміни «безпека інформації» та «безпека інформаційних технологій». Забезпечення безпеки інформаційних технологій являє собою комплексну проблему, яка охоплює правове регулювання використання ІТ, удосконалення технологій їх розробки, розвиток системи сертифікації, забезпечення відповідних організаційно- технічних умов експлуатації. Розв'язання цієї проблеми потребує значних витрат, тому першочерговим завданням є співвіднесення рівня необхідної безпеки і витрат на її підтримку. Для цього необхідно визначити потенційні загрози, імовірність їх настання та можливі наслідки, вибрати адекватні засоби і побудувати надійну систему захисту. Базовими принципами інформаційної безпеки є забезпечення цілісності інформації, її конфіденційності і водночас доступності для всіх авторизованих користувачів. Із цього погляду основними причинами порушення безпеки інформації можна назвати такі:

- несанкціонований доступ
- доступ до інформації, що здійснюється з порушенням установлених в КС правил розмежування доступу;
- витік інформації - результат дій порушника, унаслідок яких інформація стає відомою (доступною) суб'єктам, що не мають права доступу до неї;
- втрата інформації - дія, внаслідок якої інформація в КС перестає існувати для фізичних або юридичних осіб, які мають право власності на неї в повному чи обмеженому обсязі;
- підробка інформації - навмисні дії, що призводять до перекручення інформації, яка має оброблятися або зберігатися в КС;
- блокування інформації — дії, наслідком яких є припинення доступу до інформації;
- порушення роботи КС - дії або обставини, які призводять до спотворення процесу обробки інформації.

Причини настання зазначених випадків такі:

- збої обладнання (збої кабельної системи, перебої в електроживленні, збої серверів, робочих станцій, мережних карт, дискових систем тощо);

- некоректна робота програмного забезпечення (втрата або змінювання даних у разі помилок у ПЗ, втрати даних унаслідок зараження системи комп'ютерними вірусами тощо);
- навмисні дії сторонніх осіб (несанкціоноване копіювання, знищення, підробка або блокування інформації, порушення роботи 1С, спричинення витоку інформації);
- помилки обслуговуючого персоналу та користувачів (випадкове знищення або змінювання даних; некоректне використання програмного та апаратного забезпечення, яке призводить до порушення нормальної роботи системи, виникнення вразливих місць, знищення або змінювання даних, порушення інтересів інших законних користувачів тощо;
- неефективно організована система захисту; втрата інформації через неправильне зберігання архівних даних тощо);
- навмисні дії обслуговуючого персоналу та користувачів (усе сказане у попередніх двох пунктах, а також ознайомлення сторонніх осіб із конфіденційною інформацією) [6].

Порушенням безпеки можна вважати і дії, які не призводять безпосередньо до втрати або відпливу інформації, але передбачають втручання в роботу системи. Загалом найбільшу загрозу безпеці інформації становлять люди, тому саме їхні навмисні чи випадкові дії потрібно передбачати, організовуючи систему захисту.

Співробітники служб комп'ютерної безпеки поділяють усіх порушників на чотири групи стосовно жертви:

- сторонні, які не знають фірму;
- сторонні, які знають фірму, та колишні співробітники;
- співробітники-непрограмісти;
- співробітники-програмісти.

Межа між програмістами та простими користувачами з погляду небезпечності останнім часом стирається. Останні становлять більшість співробітників, звичайно мають базову комп'ютерну підготовку і можуть скористатися спеціальним програмним забезпеченням, яке має дружній

інтерфейс і доступне у спеціальних розділах BBS, на сайтах Інтернет та ін. Для позначення різних категорій комп'ютерних злочинців використовуються різноманітні терміни: «хакери», «пірати», «шкідники».

За даними дослідження корпорації IDG у 88 % випадків розкрадання інформації відбувається через працівників фірм і тільки 12 % — через зовнішні проникнення із застосуванням спеціальних засобів. Шкідники намагаються реалізувати у кіберпросторі свої патологічні схильності — вони заражають його вірусами, частково або повністю руйнують комп'ютерні системи. Найчастіше вони завдають шкоди без якої-небудь вигоди для себе (крім морального задоволення). Часто спонукальним мотивом є помста. Іноді шкідника надихає масштаб руйнівних наслідків, значно більший за можливі позитивні успіхи від аналогічних зусиль. Слід також зупинитись ще на одній групі, яка посідає проміжне місце між хакерами і недосвідченими користувачами (до речі, ненавмисні дії останніх можуть призвести до не менш тяжких наслідків, ніж сплановані атаки професіоналів). Ідеться про експериментаторів («піонерів»). Найчастіше це молоді люди, які під час освоєння інструментальних та інформаційних ресурсів Мережі і власного комп'ютера бажають вчитися тільки на власних помилках, відштовхуючись від того, «як не можна». Основну частину цієї групи становлять діти та підлітки. Головною мотивацією у цій групі є гра. З експериментаторів виходять професіонали високого класу, зокрема й законослухняні. Отже, одними з основних причин порушення безпеки інформації є незапитаність творчого потенціалу в поєднанні з неусвідомленням усіх наслідків протиправних дій. Цей фактор існує незалежно від національності або сфери професійної діяльності. Звичайно, жодна з особистих проблем не може стати приводом для протиправної діяльності, але сьогодні суспільство тільки починає виробляти належне ставлення до комп'ютерних злочинців. Стають відомими колосальні збитки від їхньої діяльності. Поширюється думка про те, що комп'ютерний злочин легше попередити, ніж потім розслідувати. Однак це не вирішує проблему повністю, адже, крім бажання розважитись і самоствердитись існує ще недбалість, холодний комерційний розрахунок, прояви садизму та хворобливої уяви. Тому комп'ютерні злочини залишаються

об'єктом уваги фахівців [6].

Більшість компаній знають, що «злом даних відбувається постійно». Однак існує також різниця між «знати» та «знати ». Коли ви занурюєтеся в дані, пов’язані з порушеннями, аргумент на користь виявлення вкрадених даних стає більш переконливим.

Відповідно до звіту про загрози Sophos 2021 :

- 97% генеральних директорів і технічних директорів погодилися, що накази про перебування вдома в 2020 році прискорили перехід на хмарні технології.
- 70% із 3700 опитаних IT-фахівців стверджували, що їхня організація зазнала порушення даних.

Згідно зі Звітом про розслідування порушень даних за 2021 рік , із 191 порушення, що виникли через «різні помилки»:

- 20% респондентів знадобилися «місяці» на відкриття
- 10% респондентів знадобилися «тижні», щоб дізнатися
- 30% респондентів знайшли «дні», щоб виявити
- 10% респондентів знайшли «хвилини», щоб виявити
- Менше 5% респондентів знадобилися «секунди», щоб виявити

Коротше кажучи, 60% респондентів витратили від «днів» до «місяців», щоб виявити збій даних. Чим довше загрози перебувають у системах, тим більше даних вони можуть вкрасти. Ось чому організаціям необхідно мати кілька стратегій і технологій виявлення.

1.3 Мета та завдання використання пасток в ІС організації

92 відсотки опитаних спеціалістів з IT та безпеки в усьому світі використовують антивірусне програмне забезпечення на основі сигнатур на своїх серверах, незважаючи на нездатність AV зупинити розширені загрози та цільові атаки.

Щоб переломити ситуацію, експерти з безпеки наполягають на використанні підходів, що ґрунтуються на поведінці, коли нетипова поведінка

може виявити ймовірні зловживання, незалежно від того, чи є у програмного забезпечення безпеки приклад свого «відбитка пальця» чи ні. Дослідники оновлюють підхід, заснований на поведінці, який існує протягом десятиліть.

Таким підходом є обман. Він ідентифікує зловмисника, коли він демонструє нетипову поведінку, то просто впадає в обман, наприклад, намагаючись взаємодіяти з підробленим веб-сервером, який не використовує ніхто.

Ціллю є те щоб поганий хлопець доклав більше зусиль, намагаючись проникнути всередину системи, ніж спеціаліст організації, щоб утримати його. Підходи до обману працюють на те, щоб ускладнити життя зловмисника і полегшити підприємству. При правильному використанні обман змусить кіберзлочинців витрачати все більше часу, зусиль і ресурсів, щоб прорвати ваш захист, а вам буде легше виявляти і обходитися з ними з меншими зусиллями.

Ефективні засоби для обману змінюють поведінку супротивника. Вони змушують роботу злочинця накопичуватися, не пропонуючи жодної винагороди за його проблеми. Його процеси повинні налагодитися, тому що йому доводиться мати справу з чимось, на що він не розраховував. Йому буде легше просто атакувати інший діапазон IP-адрес, які належать комусь іншому.

Обман тримає зусилля підприємства, що захищається, на керованому рівні - головоріз працював, щоб знайти IP-адреси та порти, які, здається, мають сервери та послуги, які він може отримати від атаки. Він працював над розробкою конкретних інструментів і підходів, які зазвичай виявляються ефективними для злому та крадіжки даних. Він точно налаштував свою здатність приховувати свою діяльність. Він має програми у вигляді елементів керування ActiveX або аплетів Java. Коли зловмисник запускає їх, думаючи, що вони збираються успішно зламати сайт, він фактично визначає своє місце розташування. Хоч порти оголені, але сервери та служби фальшиві. Кожен інструмент і підхід, який він знає, не дають ркзультату, нікуди не йдуть і нічого не відображають. І оскільки він атакує обман, який не має комерційного

використання, куди не звертається ніхто, крім хакерів, ви можете миттєво ідентифікувати його з першої спроби[7].

1.4 Постановка завдання

Технології запобігання — такі як засоби контролю доступу, шлюзи електронної пошти, системи виявлення/запобігання вторгнень (IDS/IPS), мережеві брандмауери, проксі-сервери та брандмауери веб-додатків (WAF) — є важливою основою кібербезпеки, але їх недостатньо. Традиційний периметр мережі, де зазвичай застосовуються багато з цих технологій запобігання, став пористим і регулярно порушується. Поширення хмарних обчислень, мобільності та використання власного пристрою та додатків, що працюють в Інтернеті, зробили ці засоби захисту периметра значною мірою неефективними. Загрози всередині мережевих рішень для виявлення загроз всередині мережі засновані на аномалії або на обмані. Виявлення аномалій Виявлення на основі аномалій створює базову лінію поведінки різних компонентів мережі — хостів, доступу до даних, мережевого трафіку, поведінки користувачів тощо. Будь-яка діяльність, яка не відповідає базовій лінії, позначається як сповіщення. Рішення на основі аномалій мають два істотних недоліки:

- Зйомка, зберігання та переробка масиву даних є складним, дорогим і трудомістким.
- Помилкові спрацьовування відбуваються з високою швидкістю, додаючи значний тягар для перевантажених команд безпеки.

Виявлення на основі обману є ефективною альтернативою виявленню на основі аномалій. Будь-який компонент корпоративної мережі — комп’ютерна система, служба, облікові дані, елемент даних тощо — можна використовувати для виявлення на основі обману. Обман не є частиною нормальної діяльності бізнесу чи мережі і виявляється лише шляхом атаки. Коли зловмисник витрачає час і зусилля, щоб знайти і отримати доступ до обману, спеціально створеного для виклику атаки, це є позитивним підтвердженням компромісу. Іншими

словами, у розв’язанні на основі обману оголошується дуже позитивна тенденція.

2. АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ ВТОРГНЕНЬ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

2.1 Honeypots

Honeypot («горщик з медом») можна вважати першою інкарнацією технології Deception, а з'явилися вони ще наприкінці вісімдесятих — на початку дев'яностих років. Honeypot - це мережевий об'єкт, єдина мета якого - залучати зловмисника та бути атакованим[8].

Honeypot не несе іншої цінності в мережі, де встановлено; з ним не ведеться жодних легітимних мережевих взаємодій. Коли його атакують, він фіксує це та зберігає всі дії атакуючого. Надалі ці дані допомагають аналізувати шлях зловмисника.

Побічною метою є затримати просування атакуючого по мережі, змусивши його витратити час вивчення хибного ресурсу.

Ханіпот може бути повноцінною операційною системою, яка емулює робоче місце співробітника або сервер або окремим сервісом(Рисунок 2.1).

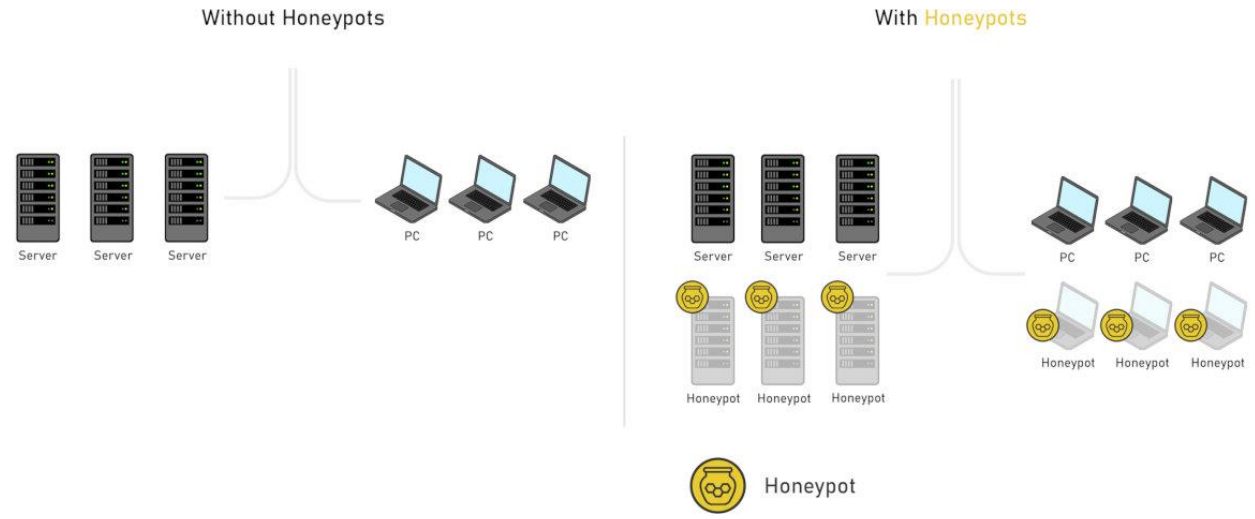

Рисунок 2.1. Порівняльне зображення мережі без пасток та з ними [8]

Теоретично, ніхто в організації не повинен взаємодіяти з пасткою. Honeypots бувають двох різновидів — з низькою та високою взаємодією — залежно від того, як задіяний нападаючий.

2.1.1 Прилади з низьким рівнем взаємодії

Приклади з низьким рівнем взаємодії засновані на емуляції частин операційної системи або мережевого стека та будь-яких необхідних служб. Ці маніпулятори відносно легко налаштувати, а емуляції не є ресурсомісткими.

Основні переваги honeypots з низьким рівнем взаємодії:

- Один комп'ютер може ефективно емулювати багато honeypot.
- Емуляції не дають зловмисникові отримати доступ до системи, уникаючи, таким чином, будь-якого ризику скомпрометації самих honeypots.

Однак приманки з низькою взаємодією обмежуються фіксацією відомої активності за допомогою відносно обмеженого набору емуляцій. Мережа підприємства зазвичай має багато складних систем, які пропонують різноманітні послуги. Навіть базова служба, така як протокол передачі файлів (FTP), зазвичай має багато версій, і одна і та ж версія може бути реалізована дещо по-різному (наприклад, налаштовані вітальні банери) у різних системах. Пристрої з низьким рівнем взаємодії пропонують лише стандартний набір мережевих послуг, а простота емуляцій (наприклад, готові відповіді, неповні емуляції тощо) полегшує противникам відбитки пальців та обходити їх.

2.1.2 Honeypots з високою взаємодією

Honeypots з високою взаємодією – це фактичні системи, а не емуляції. Вони ідентичні звичайним корпоративним системам, працюють під керуванням реальних операційних систем, пропонують реальні послуги — і потенційно надають доступ до входу зловмисникам. Проте будь-які дані в маніпуляторі з високою взаємодією є фальшивими, а операційна система та служби обладнані інструментами для детального опису дій зловмисника в системі. Honeypot також зазвичай підключається для захоплення всього мережевого трафіку, таким чином надаючи детальні дані про атаки, які можуть допомогти зрозуміти наміри зловмисника, які системи скомпрометовані, які експлойти використовуються та як налаштована інфраструктура командування та контролю (C2) [7].

Недоліки приміщень високої взаємодії полягають у тому, що вони дорогі (оскільки це реальні системи) і їх важко налаштувати, розгорнути та обслуговувати. Потрібні значні зусилля, щоб змінити природу маніпулятора високої взаємодії, наприклад, щоб забезпечити оновлену операційну систему, змінити послуги або створити підроблені дані. Оскільки зловмиснику дозволено доступ до honeypot, існує також ризик того, що honeypot може бути скомпрометований та використаний для запуску атак на інші системи чи мережі. Однак для підприємства, яке має розуміти цілеспрямовані атаки та влаштувати належний захист, немає кращої альтернативи приманкам із високою взаємодією[8].

Перше покоління технологій обману — honeypots — успішно продемонструвало ефективність обману як частини багатошарової стратегії безпеки. Проекти з відкритим кодом, особливо Honeyd і Honeynet, дозволили організаціям експериментувати з honeypots. Однак потреба в рішеннях для обману на рівні підприємства породила кілька проблем із цією першою ітерацією, включаючи наступне:

- Низька взаємодія або висока взаємодія: рішення для обману підприємства потребують як масштабу, так і здатності забезпечити детальне розуміння атак.
- Низька взаємодія на основі емуляції: простота емуляції дозволяє легко отримати відбитки пальців. Крім того, розробка та налаштування емуляцій відповідно до широти та характеристик послуг у кожній організації є величезним завданням.
- Статичні honeypots: Honeypot першого покоління демонструють відмінні характеристики, які ніколи не змінюються, і багато рішень з відкритим кодом мають добре розголошені відбитки пальців. Це дозволяє зловмисникам легко ідентифікувати ці приманки.
- Простота використання: Honeypots не були розроблені для великих підприємств, що робить адміністрування в масштабах непрактичним. Навіть якби налаштування меду займало всього хвилину, на встановлення тисячі медів

знадобилося б більше 16 годин! Зберігати honeypots було майже неможливо, і зловмисники могли легко ідентифікувати їх, оскільки вони були статичними.

- Honeypots є єдиним типом обману: ефективний обман має бути в кожній частині корпоративної мережі і поширюватися на файли, електронні листи, кешовані облікові дані, спільні ресурси мережі, бази даних, маршрутизатори, принтери тощо.
- Автономний продукт: Honeypots в основному є окремими продуктами і не взаємодіють з екосистемою безпеки, яка зазвичай присутня в будь-якій корпоративній мережі.
- Аналіз загроз. Прилади з високою взаємодією використовуються в основному для захоплення шкідливих програм, хоча були досягнуті певні досягнення у вивченні моделей атак та ідентифікації інфраструктури [1].

Виявлення, залучення та реагування на розширені загрози. Ефективне пом'якшення розширених загроз вимагає детального розуміння тактики, техніки та процедур (TTP) загроз. Рішення для обману повинні взаємодіяти із загрозами на трьох рівнях, щоб забезпечити ефективне виявлення та пом’якшення:

- Виявлення: будь-який доступ до обману виявляє загрозу з високим ступенем довіри. Обманом може бути фальшива привілея, вставлена в кінцеву точку, фальшивий спільний ресурс мережі, сервер honeypot або будь-який імітований ресурс.
- Взаємодія: коли виявлено загрозу, обман переходить у фазу взаємодії і починає взаємодіяти із загрозою для збору інформації. На етапі залучення збираються детальні TTP-загрози, зокрема корисне навантаження, експлойти бічного переміщення, центри командування та управління (C2), зламані облікові записи та цілі атаки.
- Відповідь: розуміння прийомів і цілей зловмисника допомагає як перешкодити прогресу атаки, так і закрити всі експлойти. Для цього потрібні автоматизовані розвідувальні дані для співвіднесення TTP загроз, зібраних на етапі взаємодії, і розробки відповідної стратегії реагування. Наприклад, типовою відповіддю може бути закриття доступу до зовнішніх сайтів ексфільтрації [1].

Honeypot на основі емуляції з низьким рівнем взаємодії може здійснювати лише виявлення. Він не може ідентифікувати всі використані TTP. Залучення необхідне для повного усунення загрози. Система виявлення зосереджена на пошуку зловмисників або зловмисного програмного забезпечення, які обійшли традиційні засоби захисту периметра. Виявлення не замінює захист периметра, а забезпечує додатковий рівень захисту. Думайте про цю концепцію, як про свій будинок. У вас, безсумнівно, є замки на зовнішніх дверях, але ви також можете використовувати датчики руху для виявлення небажаних зловмисників у вашому домі. Як і датчики руху, рішення для виявлення забезпечують видимість несанкціонованої та небезпечної діяльності у вашій мережі. Розгортання системи виявлення у вашій мережі являє собою зміну парадигми від традиційних моделей корпоративної мережі «повної довіри», за яких організації мають обмежену видимість незвичайної або несанкціонованої діяльності, коли користувачі отримують доступ. Навіть моделі мережі з «нульовою довірою», які забезпечують контроль доступу між різними сегментами (або зонами) мережі, зазвичай забезпечують обмежену видимість у межах окремих сегментів мережі. Використання всеосяжного обману Обман має багато форм для виявлення та залучення загроз на кожному кроці ланцюга знищення [9].

Обман можна поділити на чотири типи:

- Приманки: приманка – це сфабрикована система або програмна служба, яка є привабливою метою для зловмисника. Медовий горщик – це різновид приманки. Інші типи приманок включають маршрутизатори, принтери, служби баз даних тощо. Приманка зазвичай є більш привабливою для зловмисника, ніж сусідів виробничої мережі, тому що вона засіяна цікавими (але фальшивими) даними, а відомі вразливості залишаються відкритими.
- Панірувальні сухарі: панірувальні сухарі використовуються, щоб привести нападника до приманки. Вони важливі, оскільки початковий компроміс зазвичай є кінцевою точкою підприємства. Коли зловмисник проводить розвідку, хлібні крихти на кінцевих точках і в мережі вказують на приманки як на цікаві цілі.

- Приманки: приманки — це медові маркери — наприклад, підроблені дані або підроблені облікові дані служби — які зловмисник вважає цінними. Приманки ретельно укладаються, щоб звичайні IT-процедури або нормальна поведінка користувача їх не торкалися. Атаку можна виявити, відстежуючи доступ або використання приманки.

- Приманки: приманка робить приманку, хлібну крихту або приманку більш привабливою, ніж фактичні мережеві активи підприємства. Наприклад, щоб зробити приманку програмної служби привабливою, її можна встановити з заводськими обліковими даними за замовчуванням. Файл, який використовується як приманка, може містити сфабриковані фінансові дані. Повний обман необхідний, щоб порушити кожен із етапів ланцюга знищення після встановлення початкової точки опори під час атаки [10].

Ось кілька прикладів обманів, які можуть порушити ланцюг знищення:

- Підвищити привілеї: підроблені облікові дані користувача в кешах операційної системи (приманка)

- Внутрішня розвідка: протокол передачі файлів (FTP), протокол віддаленого робочого стола (RDP), посилання Secure Shell (SSH) та облікові дані, які спрямовують зловмисників на маніпулятори (хлібна крихта)

- Переміщення вбік: підроблені мережеві акції та приманки (приманка)

- Повна місія (вилучення даних): підроблені файли даних у приманках (приманка)

2.2 Deception

Deception відноситься до рішень класу Intrusion Detection System (IDS) - систем виявлення вторгнень. Основна мета такої системи – виявляти спроби небажаного доступу до мережі. Іншими словами, Deception допомагає виявляти мережеві атаки.

У чому відмінність Deception від ханіпотів? Ханіпот - це окремий мережевий ресурс, який ні з ким не взаємодіє, а тільки чекає на атакуючого, щоб

записати його дії. Deception - це централізована система управління помилковими мережевими об'єктами, які прийнято називати пастками (decoys). Кожна пастка є, власне, окремий ханіпот, проте вони, як показано на рисунку 2.2, пов'язані з центральним сервером [8].

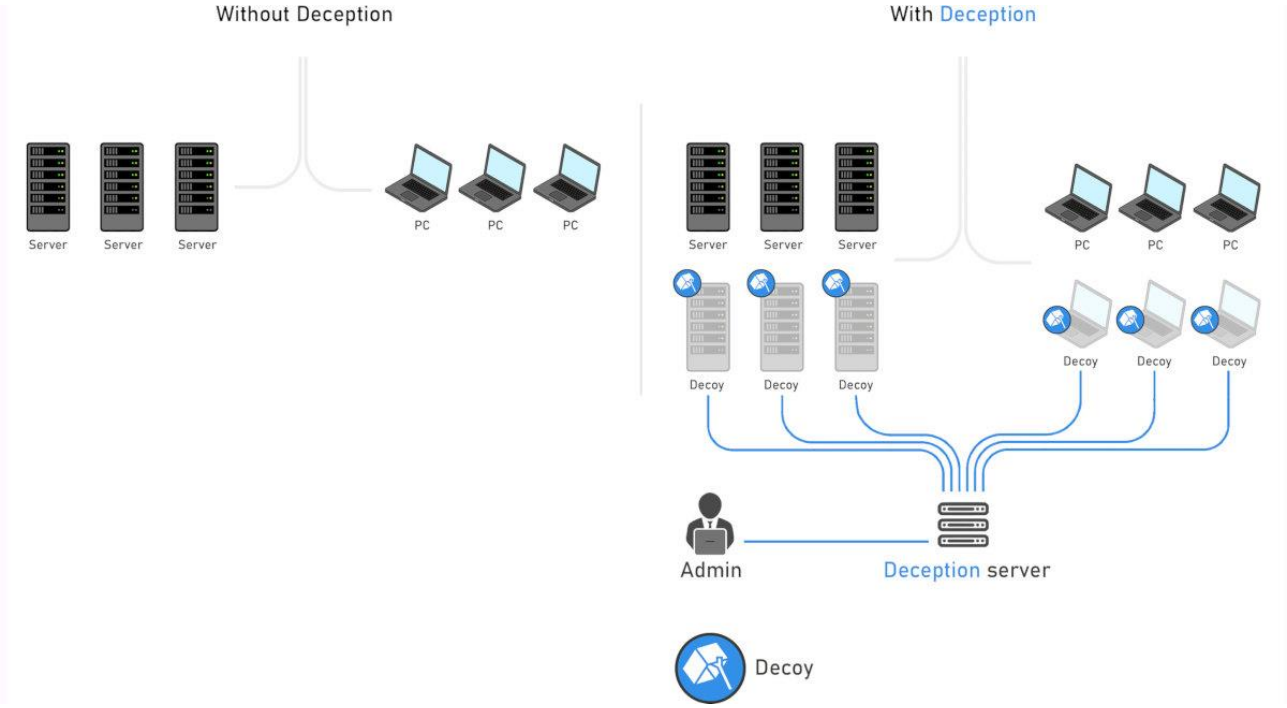

Рисунок 2.2. Інформаційна система організації без та з присутньою системою Deception [8]

Такі рішення зазвичай мають зручний інтерфейс для керування пастками. Оператор може створювати пастки з бажаним набором емульованих мережевих сервісів у вибраній підмережі, з потрібним способом отримання IP-адреси і так далі.

Пастки та емульовані ними послуги підтримують постійне з'єднання з сервером. Так само як і ханіпоти, пастки в Deception не передбачають легітимної мережевої взаємодії (за винятком взаємодії з іншими компонентами Deception)(Рисунок 2.3).

Пастка повідомлятиме сервер про будь-яку спробу взаємодії з нею: це служить індикатором атаки. При цьому оператор може моментально отримати повідомлення про подію, що відбулася. У ньому будуть вказані деталі події: адреса та порт джерела та мети, протокол взаємодії, час спрацьовування тощо.

Додаткові модулі у складі Deception можуть надавати можливість ручного або автоматизованого реагування на інциденти [8].

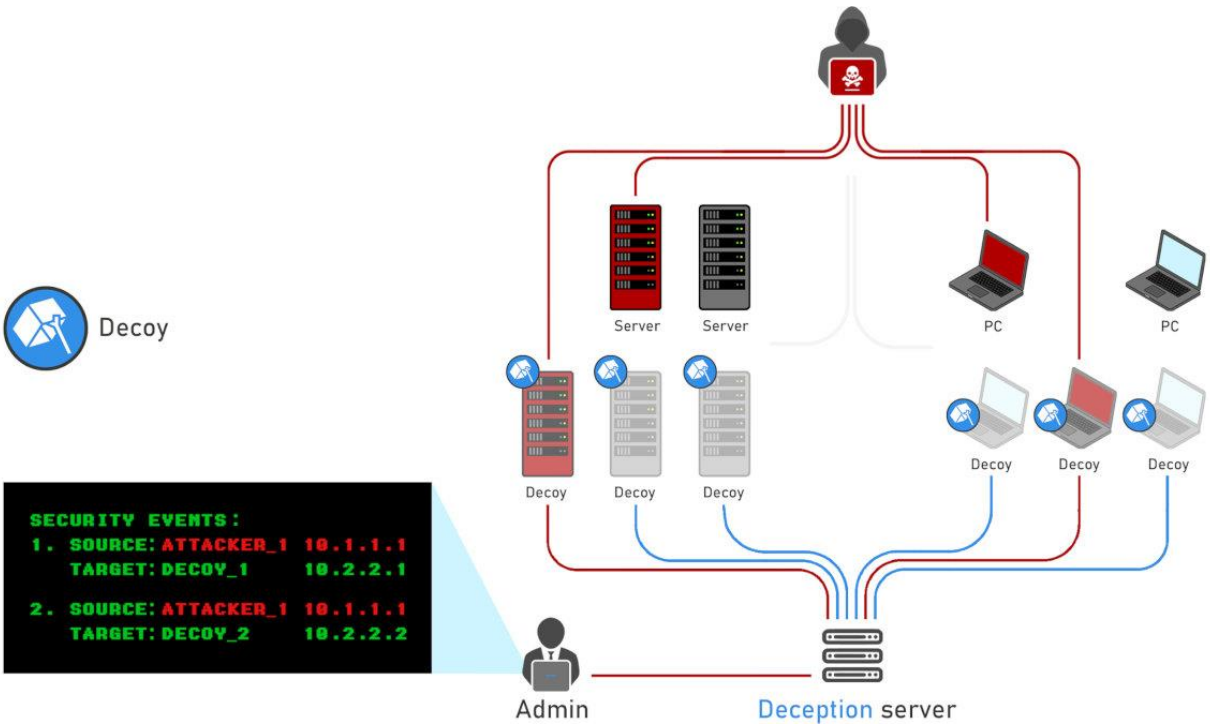

Рисунок 2.3 Реакція системи на стороннє втручання

До поняття Deception можуть входити й інші речі. Деякі компоненти допомагають спростити налаштування та автоматизацію розгортання, інші роблять пастки більш схожими на справжні мережеві сервіси, ще одні – привертають увагу хакерів до хибних цілей.

Деякі компоненти можуть вирішувати суміжні завдання, наприклад, реагувати на інциденти, збирати індикатори компрометації з робочих станцій та шукати на них вразливе ПЗ.

2.2.1 Як працює обман

Колись вважалося, що технологія призначена лише для великих організацій зі зрілими командами безпеки, однак платформи для обману перетворилися на практичне та ефективне рішення для компаній будь-якого розміру.

Компанії шукають кіберобман для комплексного захисту поверхні атак, раннього виявлення та кращого розуміння своїх супротивників. Платформи для обману задовольняють ці потреби завдяки масштабованості розгортання, простоті використання для операторів і здатності безперебійно працювати з уже наявними рішеннями безпеки.

На відміну від рішень для управління інформацією та подіями безпеки (SIEM), які використовують журнали подій для повідомлення про те, що сталося, обман проактивно повідомляє про те, що може статися. Обман ґрунтується на методах виявлення та покладанні на підписи чи відповідність шаблону, що також призводить до його ефективності [11].

Технологія обману сповіщає про раннє виявлення, розвідку та ескалацію привілеїв. Захисники можуть встановлювати приманки та приманки, приховувати виробничі активи та направляти зловмисників дезінформацією, яка зірве їх атаку. Приманки імітують справжні IT-активи по всій мережі та працюють як у реальному, так і в емульованій операційній системі (ОС). Приманки надають послуги, спрямовані на те, щоб зловмисник подумав, що він знайшов уразливу систему. Технологія також може зменшити поверхню атаки, виявляючи та виправляючи відкриті облікові дані, які створюють шляхи атаки [12].

Після взаємодії зловмисника з оманливим активом команда безпеки отримає високоточне сповіщення на основі взаємодії зі зібраними розвідувальними даними про атаку. Отримавши уявлення про інструменти, методи та наміри нападника, захисник матиме необхідні знання, щоб припинити атаку, посилити загальні стратегії захисту та зрівняти ігрове поле зі своїм суперником.

Зловмисник також отримає незрозуміле уявлення про поверхню атаки, що сповільнить їх, змусить робити помилки, витрачати додаткові ресурси та негативно вплинути на економіку атаки.

Для компаній, які проводять оцінку безпеки, технологія обману відіграє важливу роль у ранньому виявленні зловмисника та фіксації активності атаки. Ці можливості роблять технологію обману одним із найефективніших методів

боротьби з програмним забезпеченням- вимагачем . Він особливо вправний у виявленні зловмисників, які намагаються рухатися збоку всередині мережі - навіть якщо зловмисники використовують справжні облікові дані [11].

2.2.2 Реалізація

Технологія Deception доступна у вигляді повної обманної тканини або платформи, як функції в рамках більш широкої платформи та як незалежні рішення. Розширені платформи для обману використовують машинне навчання для швидкого та точного розгортання та операцій, не порушуючи інших функцій мережі. Інтеграція рідної платформи з існуючою інфраструктурою безпеки може забезпечити безперебійний обмін інформацією про атаку та сприяти автоматизації. Переваги включають автоматичне блокування, ізоляцію, пошук загроз, повторювані посібники, які прискорюють реагування на інциденти та інтеграцію з рішеннями SOAR .

Найсучасніші платформи для обману також забезпечать технологію приховування, яка приховує та забороняє доступ до даних. Замість того, щоб переплітати оманливі активи між виробничими активами, технологія може приховати реальні активи від зловмисника. Він також може повертати підроблені дані зловмиснику, щоб зірвати та збити подальші атаки. Покриття включає об’єкти AD, облікові дані, файли, папки та знімні диски, а також мережеві та хмарні спільні ресурси. Ця функція слугує потужним засобом стримування програм-вимагачів, оскільки зловмисники не можуть знайти й отримати контроль над доменом, зашифрувати чи викрасти дані на дисках, до яких вони не мають доступу [11].

Агент – це програма, яка встановлюється на реальні робочі станції користувачів чи сервери. Вона вміє спілкуватися із сервером Deception, виконувати його команди або передавати до центру управління корисні дані(Рисунок 2.4) [8].

Серед рішень класу Deception є як продукти, до складу яких входить агент, і ті, які обходяться без нього.

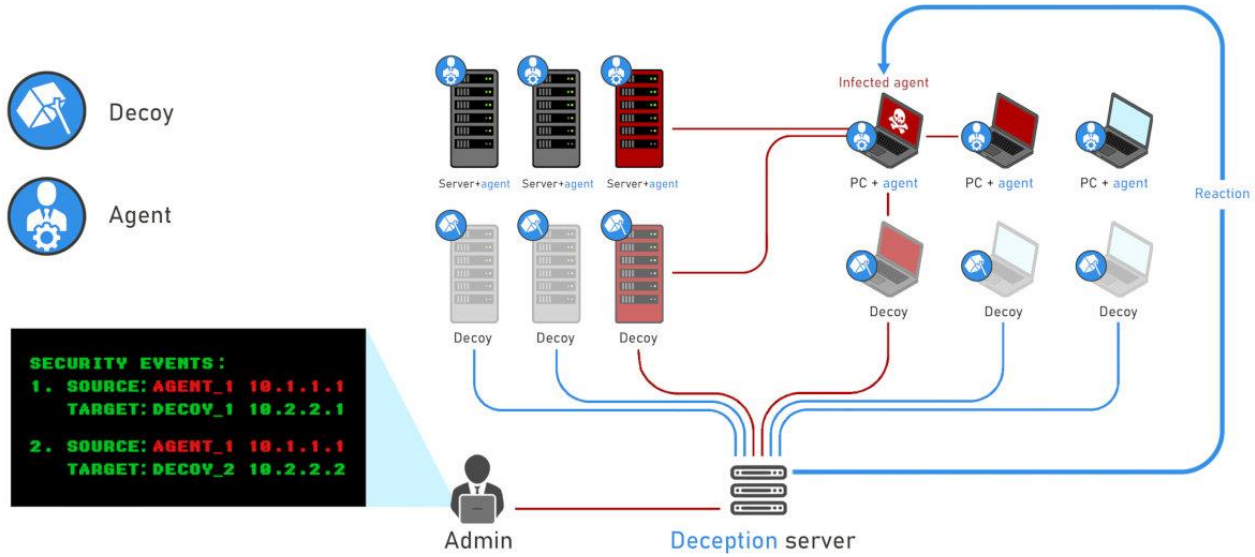

Рисунок 2.4. Приклад системи зі встановленими агентами [8]

У завдання агенту може входити:

- збирання даних про стан робочих станцій;
- поширення приманок;
- емуляція активності у мережі;
- реагування на інциденти (ручне чи автоматизоване);
- збирання даних для форензики;
- щось ще — у міру потреб клієнтів та фантазії розробника.

Діяльність агента є сенс зробити прихованою від людини, яка працює за комп'ютером. Навіщо? По-перше, користувач може навмисно або випадково видалити агент або його складові.

По-друге, наявність невідомого (або відомого до певної міри - якщо користувач про це попереджений) на робочій станції ПЗ може викликати відчуття дискомфорту.

По-третє, все, що бачить користувач, побачить і атакуючий, який одержав доступ до цього комп'ютера. Адже ми не хочемо розкрити свої карти перед атакуючим, правда?

Тому агентські рішення у складі Deception слід робити таким чином, щоб користувач не бачив ані агента, ані слідів його життєдіяльності (або хоча намагатися звести це до мінімуму).

Тому агенти зазвичай працюють у привілейованому режимі, як драйвера для Windows чи модуля ядра у разі Linux. Це дозволяє, наприклад, перехоплювати системні виклики для забезпечення скритності, а також не дає користувачеві видаляти агент або заважати працювати.

2.2.3 Переваги

Кіберобман доповнює існуючі засоби контролю безпеки, виявляючи виявлення, бічне переміщення, ескалацію привілеїв і збирання дій, для вирішення яких інші інструменти не призначені. Ця технологія дуже масштабована, що дозволяє їй захищати поверхню атаки, що постійно розвивається.

Багато видів атаки, які надає обман, традиційно важко виявити. До них належать бокове переміщення, крадіжка та повторне використання облікових даних, розвідка внутрішньої загрози, діяльність «людина посередині» (MiTM) та атаки на служби каталогів, такі як Lightweight Directory Access Protocol (LDAP) або AD.

Здатність обманювати, спрямовувати та відводити супротивника від критичних активів, позбавляє його цілей і показує, як вони хочуть рухатися через мережі. Це також дає перевагу збільшенню вартості зловмисника, оскільки тепер він повинен розшифрувати реальне від того, що є підробкою, і змушує їх перезапустити свої атаки.[11]

2.1 Аналіз існуючих рішень

Кілька років тому багато компаній, що займаються технологіями обману, додавали такі передові функції, як хмарна інтеграція, штучний інтелект та автоматизація, на свої платформи для боротьби зі все більш

розвиненими загрозами. Оновлений захист був необхідний, оскільки досвідчені зловмисники починали демаскувати й обходити класичні хитрощі обману, як-от кидання хлібних крихт, що вказують на фіктивні, статичні активи. Сьогодні технологія обману знову має перевагу і може розгорнути лабіринт реалістичних, але підроблених активів, які дуже схожі на справжні.

Покращені зусилля, спрямовані на заманювання та в кінцевому підсумку захоплення навіть найдосконаліших хакерів, керуються кількома компаніями, які мають платформи для обману в авангарді цієї технології, яка все ще розвивається. Нижче наведено низку інноваційних інструментів для обману, доступних на сьогодні.

2.3.1 Acalvio Shadowplex

Платформа Shadowplex від Acalvio була розроблена з нуля для використання в корпоративних середовищах. Компанія не просто розглядає типові IT-пристрої, такі як комп’ютери, принтери та файлові сервери, як частину цього потенційного підприємства. Shadowplex також може захистити датчики та пристрої Інтернету речей (IoT) і навіть промислові центри управління, які складають більшу частину ландшафту операційних технологій (OT) [13].

У випадку як IoT, так і OT-пристроїв, наявність рівня технології обману для їх захисту є критичною, оскільки багато з них мають обмежену або не мають вбудованої безпеки самостійно. Це також робить його хорошим вибором для чогось на кшталт середовища охорони здоров’я, де він може імітувати такі речі, як настільні комп’ютери разом із медичними пристроями, заманюючи зловмисників у будь-який з них, залежно від їх інтересів.

Можливість захисту IoT і OT вражає, але Shadowplex примітний тим, як він справляється з масовими розгортаннями обману в масштабі, не використовуючи занадто багато ресурсів. Секрет полягає в тому, що всі активи для обману існують всередині так званої ферми обману, яка може бути розташована всередині хмари або локально у віртуалізованій фермі серверів.

Щоб підключитися до фізичної мережі, потрібна серія датчиків, які діють як кінцева точка для програмного тунелю. Датчики не повинні бути потужними або дорогими. Мережевий пристрій за 50 доларів буде працювати нормально, або він також може бути програмним та віртуалізованим. Вам потрібен один для кожного сегмента мережі, який ви захищаєте.

Принцип роботи Shadowplex полягає в тому, що віртуальні, оманливі активи розгортаються в мережі, яку вони будуть захищати. Ці активи можуть бути автоматично розгорнуті на основі хост-середовища, при цьому Shadowplex вибирає гарне поєднання операційних систем, IT, OT та пристроїв Інтернету речей. Активи для обману можуть спілкуватися один з одним і генерувати трафік, але фактично взаємодіють лише в межах ферми обману, і ці результати імітуються в реальному середовищі.

Незважаючи на те, що технічно це фасади, як тільки ворог взаємодіє з ним, центр керування AI на фермі обману негайно розкручує обманний актив, допомагаючи йому працювати так, як зловмисник очікує від настільного комп'ютера, принтера або промислового контролю. пристрій для дії. Зловмисник буде зайнятий якомога довше, а також попереджати служби безпеки про атаку. Shadowplex також представляє зловмисникові ситуації, щоб дізнатися більше про їхні наміри та тактику, що чудово не тільки для пом'якшення поточної загрози, але й для запобігання їх у майбутньому.

Не потрібно бути експертом з обману, щоб працювати з Shadowplex. Напрочуд корисні майстри в програмі будуть виконувати ставки користувача у відповідь на прості запитання та вказівки. Для такої потужної платформи наявність такого легкого інтерфейсу є справжньою перевагою.

2.3.2 Attivo ThreatDefend

Attivo був одним із перших розробників технології обману, який додав можливість реагування до свого продукту, і компанія домоглася цього ще більше завдяки своїй новій платформі Attivo ThreatDefend Deception and Response Platform . Тепер його можна розгорнути локально, в хмарі, центрах

обробки даних або гібридних мережах. Компанія постійно розвиває активи для обману на основі нових пристроїв і пропонує створювати унікальні обмани, якщо у клієнта є щось ексклюзивне всередині свого середовища. Усі розгорнуті приманки є реальними активами, які використовуються в мережі [14].

Мета платформи Attivo така ж, як і інших наборів інструментів для обману, а саме розгортання підроблених активів, з якими будуть взаємодіяти зловмисники, але які реальні користувачі або не знають, або не матимуть жодної причини торкатися. Деякі з приманок є дещо більш публічними, ніж інші, що може допомогти відшукати інсайдерські погрози або стежити за співробітниками. Здебільшого засоби для обману призначені для того, щоб ловити акторів-загроз, які пробираються через мережу і намагаються намітити шлях далі всередину, підвищити свої облікові дані, переміщатися збоку або прямо вкрасти дані.

Як тільки зловмисник взаємодіє з одним із оманливих активів Attivo, він робить більше, ніж просто генерує сповіщення, хоча він також робить це. Він також взаємодіє зі зловмисником, надсилаючи ті відповіді, які може очікувати загарбник. Він може активувати пісочницю, щоб будь-яке зловмисне програмне забезпечення або інструменти для злому, завантажені зловмисником, потрапляли в пісочницю. Це не тільки захищає мережу, але й дозволяє досліджувати зловмисне програмне забезпечення, щоб визначити намір і тактику зловмисника.

Платформа також дозволяє адміністраторам виконувати різні дії, як-от помістити систему в карантин, яка використовується зловмисником як платформу запуску, або втратити облікові дані зламаного користувача. Як тільки користувачі починають довіряти платформі, ці дії можна налаштувати на автоматичне виконання, щойно буде зібрано будь-яку важливу інформацію про загрози.

Платформа Attivo Deception and Response Platform не лише забезпечує хорошу технологію обману, але й допомагає захисникам швидко розпочати

свої можливості реагування, що є важливою перевагою у світі, де рахуються секунди.[15]

2.3.3 Fidelis Deception

Управління будь-якою мережею підприємства - важка робота. Додавання шару підроблених або оманливих активів робить це ще складніше. Все може стати набагато простіше, якщо користувачі використовують платформу Fidelis Deception , яка автоматизує більшість складніших аспектів захисту на основі обману.

Ви можете пройти через процес розгортання обманних засобів за допомогою простих у використанні майстрів і спадних меню або просто дозволити Fidelis автоматизувати все. Він чудово справляється з розгортанням активів, які відповідають будь-якому іншому середовищу. Він продовжуватиме стежити за мережею, оскільки вона розвивається та розширюється, надаючи пропозиції щодо того, як віддзеркалити ці зміни в мережі обману. Наприклад, якщо компанія додає купу нових камер безпеки IoT, Fidelis виявить це і запропонує розгорнути купу підроблених камер зі схожими характеристиками. Він повністю підтримує майже будь-який пристрій IoT, а також багато з них, які можна знайти в OT.

Крім простого розгортання, Fidelis також контролює свої підроблені активи, забезпечуючи їх зв’язком один з одним і виконанням дій, які виконував би звичайний пристрій того ж типу. Він навіть розпочинає деякі дивовижно просунуті тактики, як-от отруєння таблиці протоколу розділення адрес (ARP), щоб виглядати так, ніби оманливі активи так само активні, як і реальні, які вони захищають.

Нарешті, Fidelis унікальний тим, що він також породжує фальшивих користувачів, які реалістично взаємодіють із оманливими активами. Хакер, який намагається визначити, чи є актив справжнім, побачить докази взаємодії користувачів із ним і знехтує, не знаючи, що самі користувачі є частиною складного обману.[16]

2.3.4 TrapX DeceptionGrid 7.0

Платформа DeceptionGrid від TrapX продовжує залишатися однією з найнадійніших програм захисту від обману, особливо з точки зору кількості реалістичних, але підроблених активів, які вона може розгорнути. Для DeceptionGrid не є незвичайним розгортання тисяч і тисяч підроблених активів у мережі, яку він захищає, хоча це не обов'язково означає, що кожен із них є повністю функціонуючим оманливим пристроєм.

Оманливі активи, розгорнуті DeceptionGrid, включають звичайні мережеві пристрої, маркери обману та активні пастки. Починаючи з більшості розгортань, основні оманливі засоби створені так, щоб виглядати як повністю функціонуючі комп'ютери або пристрої, а TrapX має кілька шаблонів, розроблених для певних галузей, як-от фінансовий сектор або охорона здоров'я. Він може імітувати все, починаючи від банкомату і закінчуючи торговельним обладнанням і майже будь-яким активом Інтернету речей. Крім того, DeceptionGrid може розгортати оманливі активи з повними операційними системами. Вони називаються пастками FullOS і призначені для того, щоб зловмисник повірив, що він працює з реальним активом, одночасно повністю відстежуючи все, що вони роблять для збору інформації про загрози.

Менші, але настільки ж важливі маркери обману, які розгортає TrapX. На відміну від повнофункціональних оманливих активів, токени — це звичайні файли, скрипти конфігурації та інші види приманок, які зловмисники використовують для збору інформації про системи та мережі, які вони намагаються зламати. Вони не будуть взаємодіяти зі зловмисником, але сповіщатимуть команди безпеки щоразу, коли до них доступ, копіювання чи перегляд.

Активні пастки доповнюють обсяг оманливих активів, розгорнутих DeceptionGrid. Ці пастки передають між собою обсяги фальшивого мережевого трафіку з вказівниками та підказками, які ведуть назад до решти мережі обману. Будь-який зловмисник, який тихо стежить за мережевим трафіком, швидше за все, буде обдурений фіктивним мережевим потоком, що

приведе його до оманливого активу, навіть якщо він, ймовірно, припускає, що він безпечний, оскільки виглядає так, ніби він регулярно й повноцінно використовується в мережі.

Якщо ви хочете покрити свою мережу армією оманливих засобів для повного захисту, ніщо не може допомогти досягти цієї мети краще, ніж TrapX DeceptionGrid. Це не зовсім тонко, але для зловмисника майже немає способу успішно переміщатися через складний лабіринт різноманітних обманних засобів, які може розгорнути DeceptionGrid[17].

2.3.5 ThreatDefend

Платформа ThreatDefend забезпечує вкрай необхідне рішення для виявлення для сучасних сучасних команд безпеки будь-якого розміру. Поточний такі інструменти, як SIEM, надають великі обсяги даних, які потребують виділеного часу та ресурсів для відокремлення помилкових результатів фактичні інциденти безпеки. Системи на основі сигнатур, такі як антивірусні засоби та засоби моніторингу кінцевих точок, можуть легко пропустити нульовий день або складні атаки. Методи поведінкової аналітики викликають втому попередження і регулярно не звертають уваги на просунутих зловмисників і інсайдерів загрози, оскільки люди-нападники не є повністю обчислюваними об’єктами. Поточні засоби контролю безпеки не можуть ефективно виявити зловмисників націлювання на Active Directory для виявлення, використання даних, бічного переміщення та підвищення привілеїв.

Платформа ThreatDefend дозволяє командам безпеки зосередитися на пошуку та реагуванні на атаки, а також надати їм видимість у нових і складну тактику, перетворюючи все IT-середовище на пастку. Крім того, висока точність і низька гучність сповіщень дозволяють система для роботи з низьким рівнем обслуговування та накладними витратами, надаючи неймовірно точні та відповідні дані про загрози. Технологія обману проста і швидко розгортається. Протягом кількох годин після встановлення Attivo BOTsink або Endpoint Detection

Мережне рішення, групи безпеки можуть проектувати тисячі автоматично налаштованих приманок і приманок через свою мережу, забезпечуючи обман і раннє оповіщення. З правильною стратегією «повзати, ходити, бігати» це може перерости в повністю інтегрований та справжній шар обману, який обдурить і вловить навіть найобережніші та зрілі загрози.

Набір продуктів Endpoint Detection Net також дозволяє організаціям створювати різні оманливі облікові дані, фальшиві об’єкти, такі як як маркери SSH, ключі хмарної платформи та спільні ресурси SMB для розміщення в існуючих виробничих системах, які повертають зловмисників до манки. Приховані картографічні акції для малого та середнього бізнесу діють як приманки для програм-вимагачів, які прагнуть поширюватися через мережеві диски, зупиняючи шкідливе програмне забезпечення безперервно передавати йому дані, одночасно регулюючи з’єднання, щоб дати командам безпеки час, щоб відповісти на них. Крім того, ASecure модуль шукає неавторизовані запити Active Directory (AD) і перехоплює результати, приховуючи чутливі чи критичні об’єкти та повертаючи на їх місце оманливі приманки. Функція Deflect також робить будь-яку кінцеву точку виробництва приманкою, яка перенаправляє атаки націлювання портів і служб у середовище обману для взаємодії, по суті, блокування кінцевих точок від зловмисника бічний рух.

Компонент ThreatPath визначає розкриття облікових даних і неправильні конфігурації на кінцевих точках, які дозволяють зловмисникам рухатися по всій мережі від системи до системи. Рішення відображає з’єднання та індексує дані для пошуку та аналіз. Виявивши такі вразливості, команда безпеки може очистити збережені облікові дані, виправити неправильно налаштовані політики, або додайте облікові дані для приманки, щоб додатково захистити кінцеві точки.

Коли зловмисник взаємодіє з середовищем обману, платформа ThreatDefend негайно повідомляє про активність для команди безпеки, щоб швидко визначити джерело атаки для автоматичного реагування на інцидент. Коли зловмисник безпосередньо звертається до приманки або взаємодія з веб-сторінкою чи загальним ресурсом для малого та середнього бізнесу, розміщеною на ній, платформа реєструє всю активність, відображаючи її команді безпеки в

панель приладів. Платформа фіксує криміналістичні дані, що надають інформацію для реагування на інцидент та дій по виправленню, в т.ч запис усього трафіку команд і управління (C2) і ведення пам'яті криміналістичний аналіз. Для служби безпеки це багатство організації- спеціальну розвідку загроз, яку вони можуть використовувати для подальшого покращення свого захисту.

Рішення ThreatDirect масштабується в локальних, віддалених офісах, і хмарні середовища. Переадресатор поставляється як віртуальна машина, модуль кінцевої точки, або контейнерний додаток. Він може працювати на кінцевих точках, серверах, ВМ середовища або комутатори, які містять гіпервізор або можуть запускати контейнер додатків. Така гнучкість розгортання приносить користь організаціям широка та різноманітна мережева інфраструктура.

Рішення DecoyDocs створює оманливі файли з вбудованою функцією маяка, яка сповіщає групи безпеки про неналежне доступ. Під час попередження в мережі рішення надає повну інформацію про хост, який отримує до нього доступ. Якщо зловмисник ексфільтрується документ, він буде маяком додому з геолокацією кожної IP-адреси, яка його відкриває. Цю можливість дає команда безпеки знання того, на що націлені зловмисники.

Повторювані підручники ThreatOps використовують численні інтеграції партнерів, вбудовані в платформу, для послідовної та автоматизований процес реагування на інцидент. Ця функція усуває складність і прискорює реагування на інциденти, полегшуючи робочі навантаження для команди безпеки, які стикаються з проблемами ресурсів.

Загалом, платформа ThreatDefend забезпечує комплексне та просте у використанні рішення для обману загроз, яке масштабується в будь-якому розмірі. мережі, незалежно від місця розташування, і прискорює реагування на інциденти, надаючи критично важливі розвідувальні дані супротивника для покращення захисту.[18]

2.3.6 Xello Deception

Технологія Xello Deception створює приманки та пастки у вигляді облікових даних користувачів, серверів, сервісів та сайтів, активно заманюючи атакуючого у щільну мережу хибних даних.

Рішення діє після того, як «традиційні» засоби захисту корпоративної мережі пройдені, але раніше, ніж зловмисники завдали шкоди компанії.

Збирайте форензику безагентським способом та розповсюджуйте приманки. Перетворіть реальні хости на мережу приманок та пасток. Використовуйте сервер-пастку з повним доступом до операційної системи.

За допомогою штучного інтелекту запатентована технологія Dexem робить приманки максимально реалістичними та невідмінними від активних активів корпоративної мережі, заганяючи зловмисника в розставлені пастки.

Автоматизуйте, керуйте всім неправдивим шаром через єдиний сервер. Інтеграція з усіма суміжними системами: Active Directory, DNS, SIEM, Email тощо

Збір та обробка подій з усіх джерел платформи та суміжних систем для моментального реагування на інцидент.

Xello Deception – це:

- Адаптивна генерація За допомогою штучного інтелекту система генерує набір хибної інформації, який є максимально реалістичним у мережі.
- Робота без агента Кіберзлочинець не зможе детектувати рішення через відсутність хостового агента.
- Інтеграція із SIEM-системами Xello Deception інтегрується з різноманітними SIEM-системами, що робить реагування та моніторинг максимально ефективними.
- Відсутність слідів роботи Вся інформація про місцезнаходження приманок та пасток зберігається в системі. За бажанням, дані можна очистити, не вплинувши на інфраструктуру і роботу мережі.[19]

3. ПОРЯДОК ЗАСТОСУВАННЯ DECEPTION-ТЕХНОЛОГІЇ ДЛЯ ВИЯВЛЕННЯ ВТОРГНЕНЬ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ НА БАЗІ РІШЕННЯ XELLO DECEPTION

Беручи до уваги все вищеперечислене вибір рішення для впровадження до ІС організації зупинився на Xello Deception. Тому розглянемо процес її розгортання більш детально.

Система Xello Deception має такі функціональні можливості:

- Централізована система розповсюдження приманок та управління ними.
- Інтеграція з EDR, NAC, пісочницями та SIEM-системами.
- Можливість створення унікальних приманок на основі даних щодо інфраструктури замовника.
- Збір та обробка подій з усіх доступних джерел для проведення розслідувань інцидентів.
- Виявлення цілеспрямованих (APT) атак у реальному режимі.
- Наявність запатентованої технології Dexem для створення реалістичних принад.
- Застосування машинного навчання та бази сценаріїв атак для оперативного виявлення дій зловмисника.
- Застосування безагентного способу роботи з принадами.

Архітектура Xello Deception Xello Deception є комплексною системою для створення розподіленої платформи хибних цілей. Вона включає кілька модулів.

- Модуль Xello Endpoint Deception є елементом системи, призначеним для збору подій безагентним способом на кінцевих точках для подальшого проведення розслідувань інцидентів та встановлення пасток та приманок.
- Модуль FullOS TRAP є сервером-спритністю з повним доступом до операційної системи.
- Модуль Xello Management Center є сервером керування та необхідний для керування всіма пастками та принадами.

- Модуль Event Collector призначений для збору та обробки подій за всіма джерелами, доступними на платформі та суміжних системах, для моментального реагування на інциденти.

Інтерфейс консолі управління підтримує три мови: російську, англійську та іспанську. Ліцензійна політика щодо Xello Deception цілком гнучка. Ліцензії можуть бути тимчасовими терміном на 1 рік, так і безстроковими. В обидва типи ліцензії входять технічна підтримка. Система ліцензується за кількістю хостів, що захищаються. Xello Deception має відкритий API для взаємодії зі сторонніми продуктами та системами, наприклад, з EDR, NAC, пісочницями. Також підтримується інтеграція з SIEM за допомогою механізмів Syslog CEF та Syslog RFC JSON.

3.1 Системні вимоги для Xello Deception

Кожен із компонентів системи Xello Deception має свої системні вимоги для встановлення, які наведено у таблиці 3.1.

Таблиця 3.1.

Системні вимоги до встановлення компонентів Xello Deception

Компонент	Вимоги до ОС	Вимоги до апаратного забезпечення	Інші вимоги
Сервер керування	Сервер керування Microsoft Windows Server 2016 (англійська локалізація) та нові	ЦП: 4 ядра ОЗУ: 8 ГБ ПЗУ: 100 ГБ	PowerShell версії 4 . SE Environment 8 Статична IP-адреса
Сервер-пастка	Microsoft Windows Server 2016 (англійська локалізація) і нові	ЦП: 4 ядра ОЗУ: 8 ГБ ПЗУ: 100 ГБ	Статична IP-адреса

Продовження таблиці 3.1

Системні вимоги до встановлення компонентів Xello Deception

Захищені хости	Microsoft Windows 7, 8, 10, Server 2012, Server 2016, Server 2019, Сімейство Linux (Ubuntu, Debian, CentOS, RHEL, Astra Linux, Alt Linux), macOS (High Sierra та новіші версії).	Рекомендовані для відповідних ОС	Увімкнений сервіс File and Printer Sharing Пінг між хостами, що захищаються, і сервером управління дозволений в обох напрямках

3.2Встановлення системи Xello Deception

Для роботи Xello Deception необхідне встановлення в інфраструктурі двох компонентів: сервера керування та сервера-пастки.

Для того щоб почати інсталяцію компонента керування, необхідно запустити файл установки «MgmtSetup.exe», який знаходиться в каталозі «Management» дистрибутива. Далі у вікні майстра установки слід ознайомитися з ліцензійною(Рисунок 3.1).

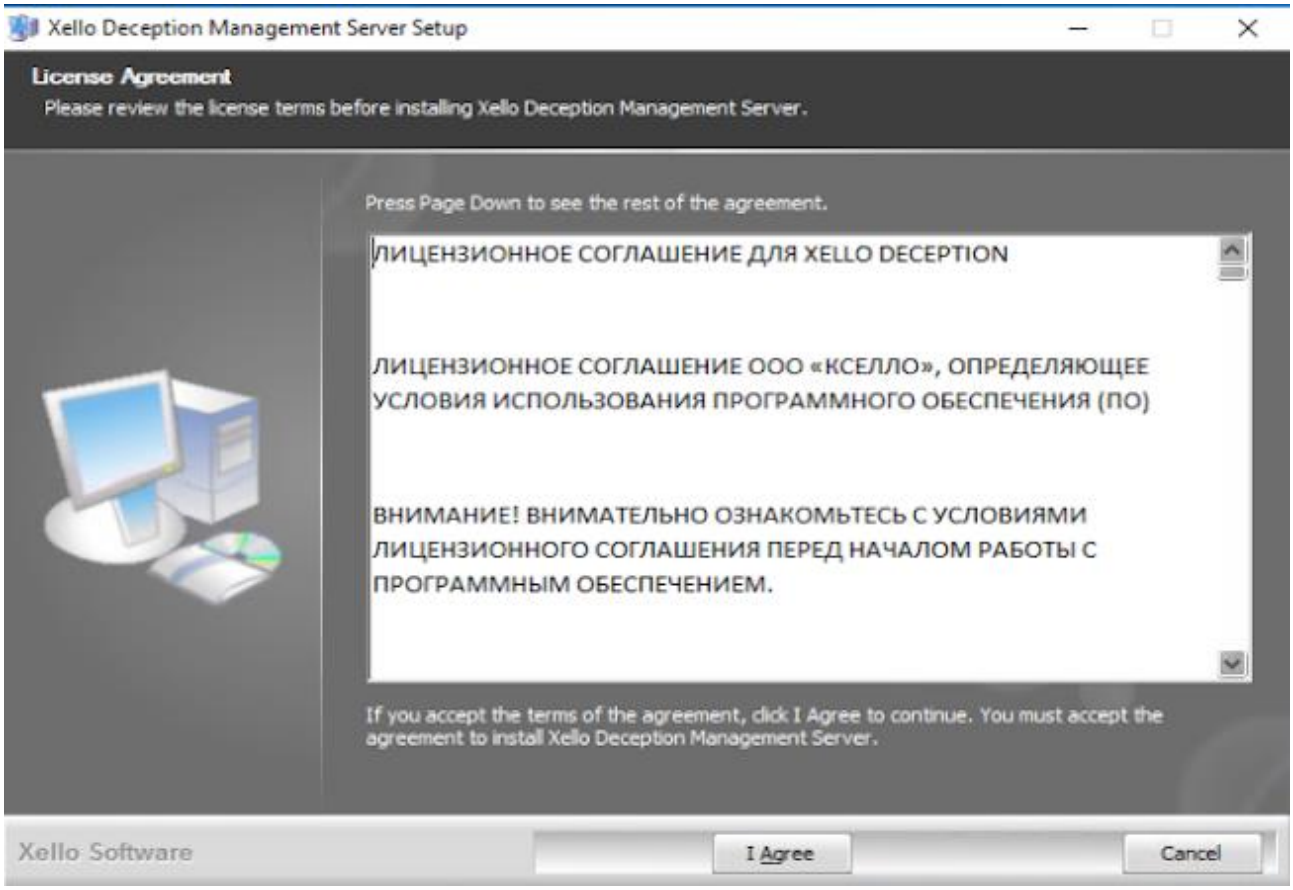

Рисунок 3.1. Встановлення сервера керування Xello Deception

На наступному етапі з'явиться нове вікно Choose Components. Слід вибрати рядок "MGMT server files" та натиснути "Next"(Рисунок 3.2).

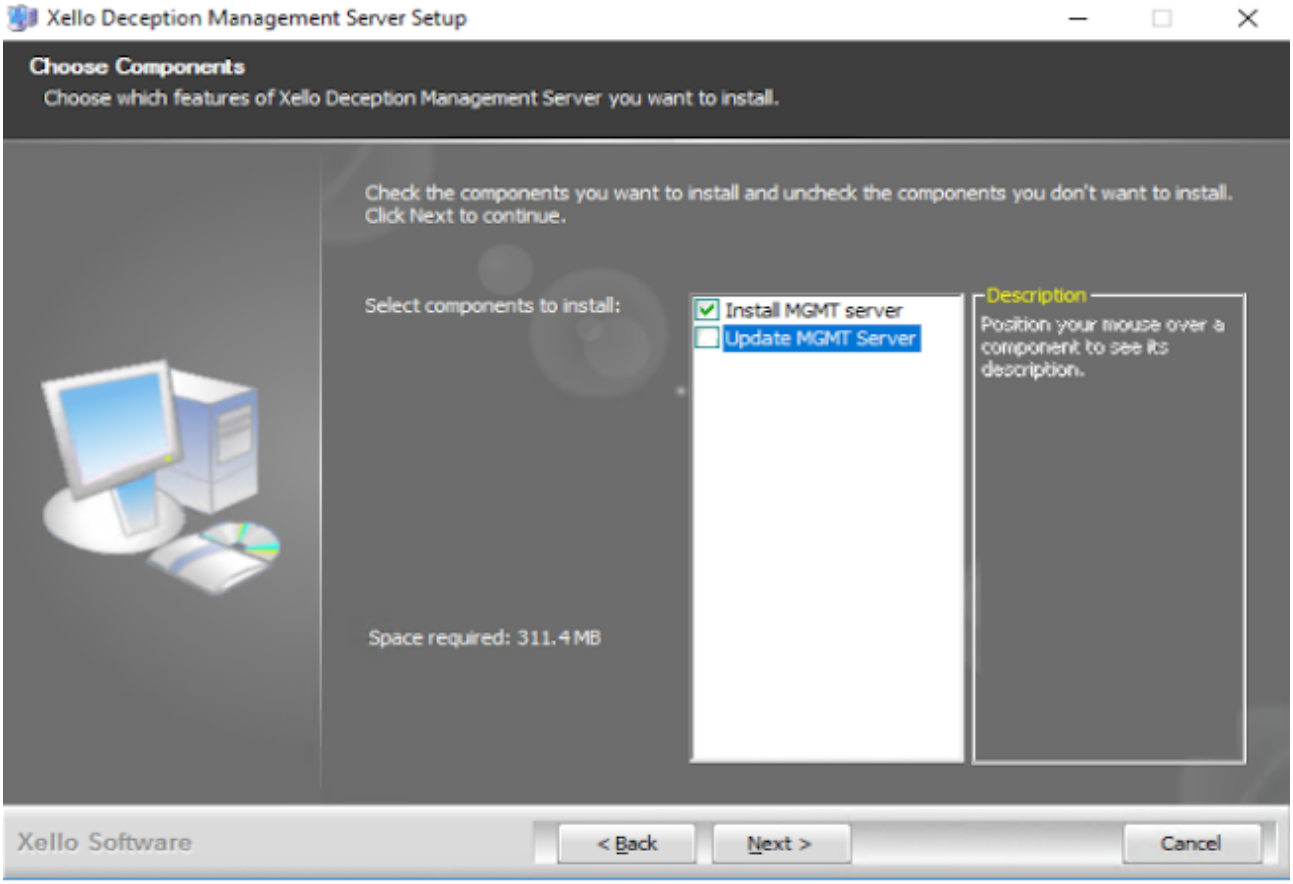

Рисунок 3.2. Вибір необхідного компонента Xello Deception у вікні Choose Components

Далі з'явиться вікно із вибором каталогу для встановлення. У вікні Choose Install Location необхідно вибрати папку і натиснути кнопку Next (Рисунок 3.3).

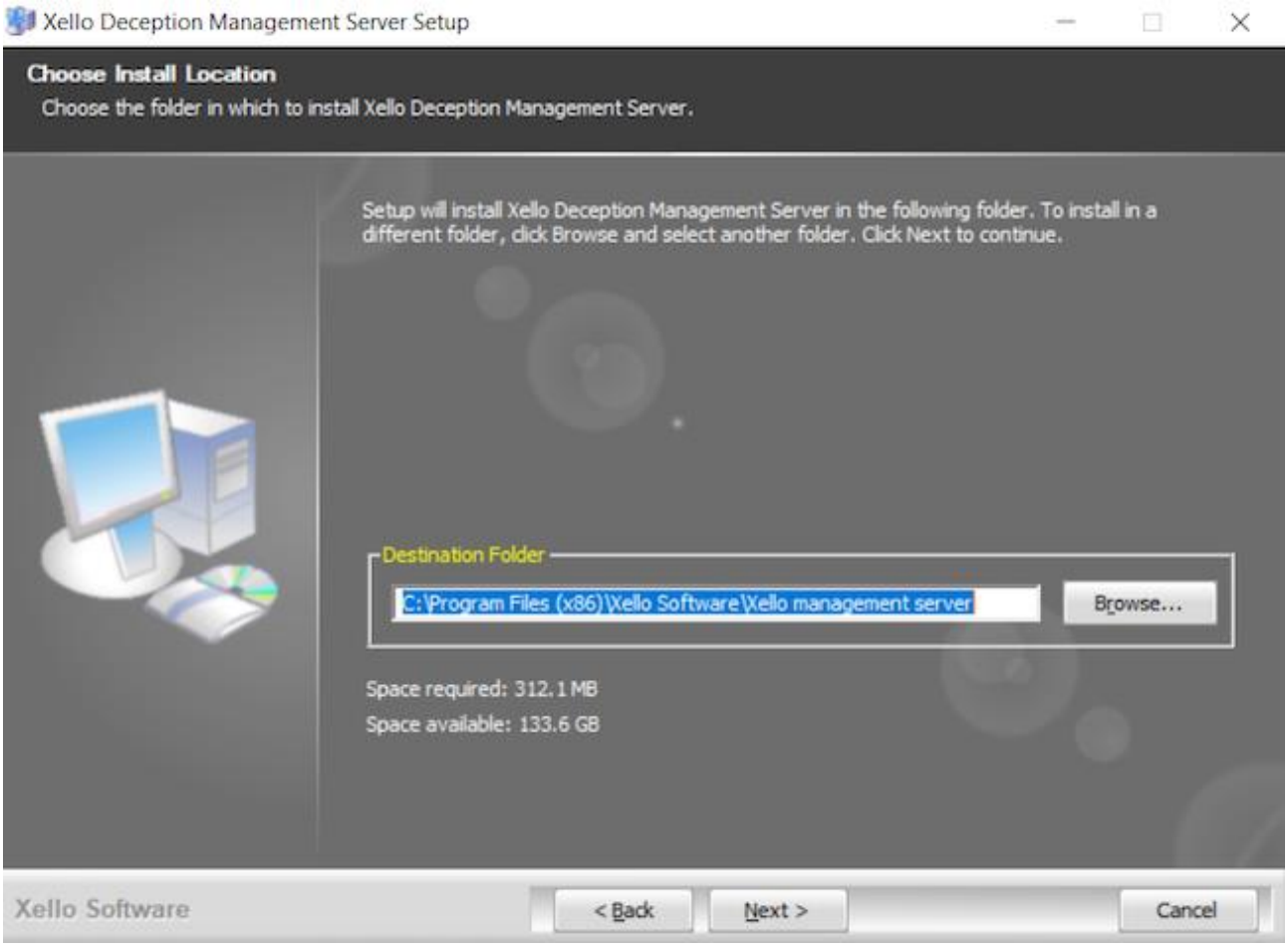

Рисунок 3.3. Вибір папки для встановлення компонента Xello Deception

На наступному етапі знадобиться підтвердити дію установки компонента і у вікні «Confirm Installation» натиснути кнопку «Install». Далі розпочнеться процес встановлення елемента системи. Після завершення цього процесу потрібно натиснути кнопку "Close" для виходу(Рисунок 3.4).

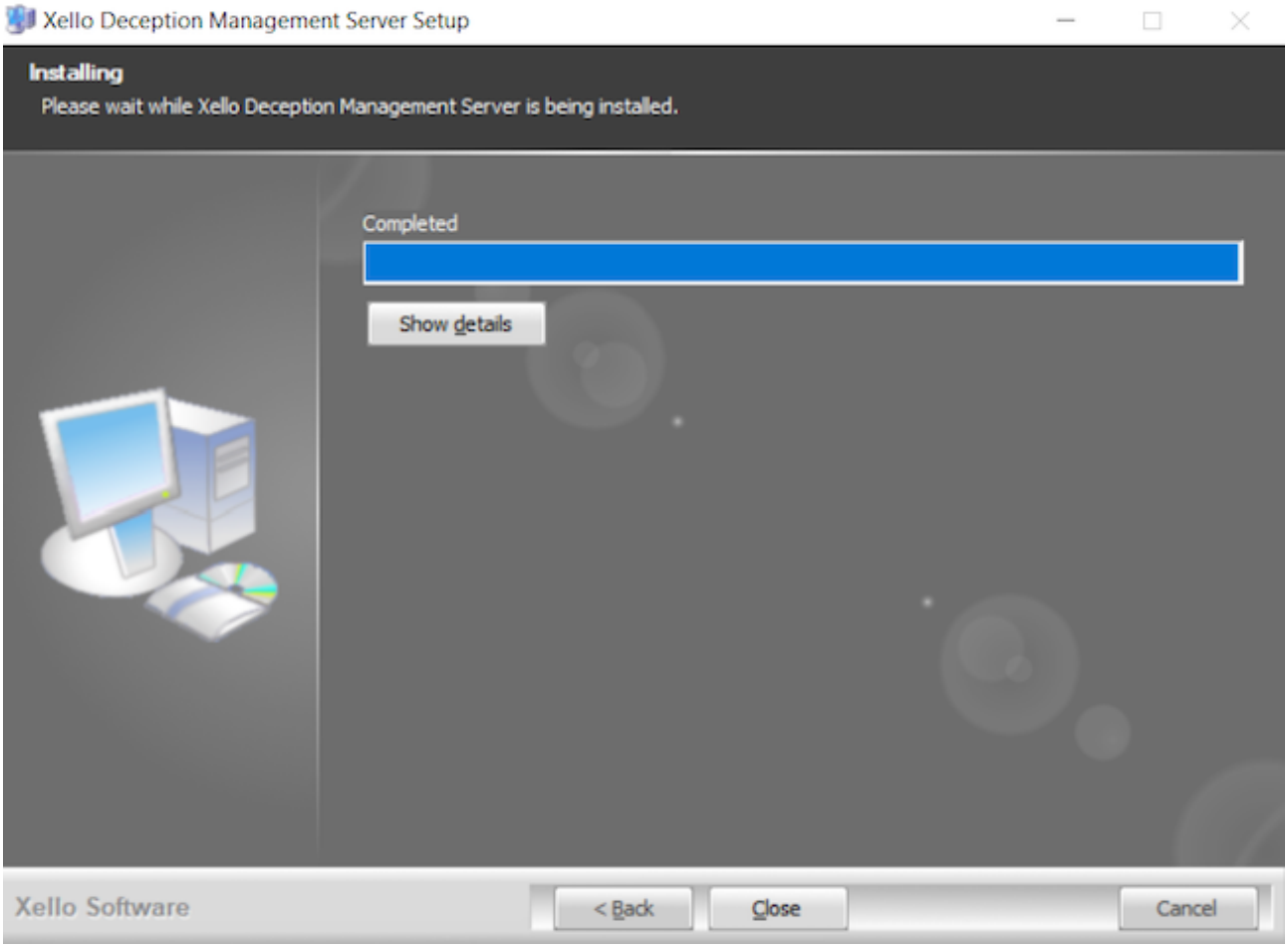

Рисунок 3.4. Завершення установки сервера керування Xello Deception

Однак процес встановлення компонента на цьому не закінчиться. Необхідно також додати утиліту PsExec з пакета Sysinternals в корінь робочої директорії Xello Management Server і потім перезавантажити сервер.

3.3 Встановлення сервера-пастки Xello Deception

Для встановлення сервера-пастки необхідно запустити файл «TrapSetup.msi», що знаходиться в каталозі «Trap» дистрибутива, що поставляється. Процес інсталяції за допомогою майстра виглядає так само, як і для сервера управління: ліцензійна угода, вибір компонентів, призначення папки, підтвердження. Після завершення встановлення з'явиться вікно для встановлення параметрів сервера-пастки. У ньому слід вказати IP-адресу сервера управління або ім'я та порт, логін та пароль користувача TrapUser, ім'я сертифіката для пастки HTTPS. Потім потрібно натиснути на кнопку "Write" для

збереження параметрів, а потім - на кнопку "Exit" для завершення установки сервера-пастки(Рисунок 3.5). Також потрібно перезавантажити сервер.

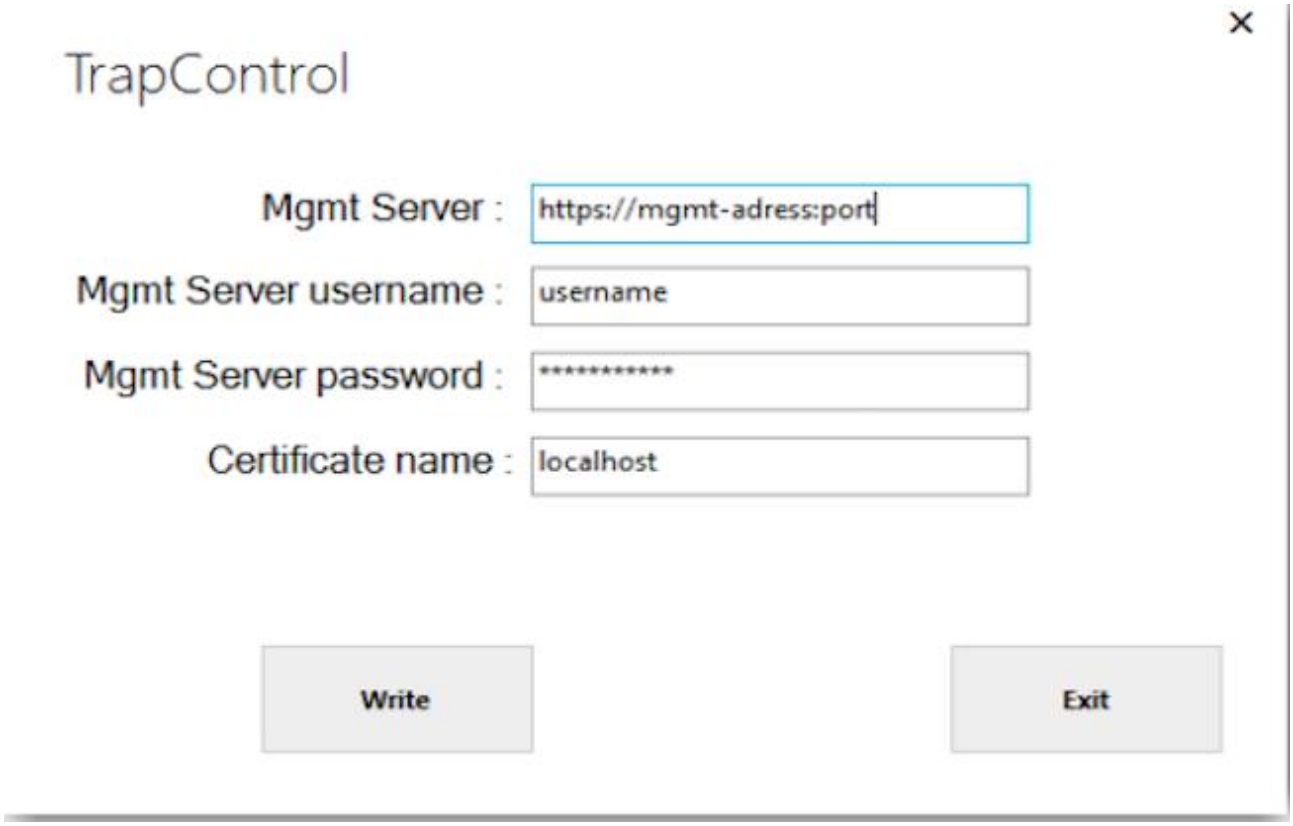

Рисунок 3.5. Встановлення параметрів роботи сервера-пастки у Xello Deception

3.4 Огляд панелі керування Xello Deception

Конфігурація системи здійснюється за допомогою консолі адміністрування через розділ "Налаштування"(Рисунок 3.6).

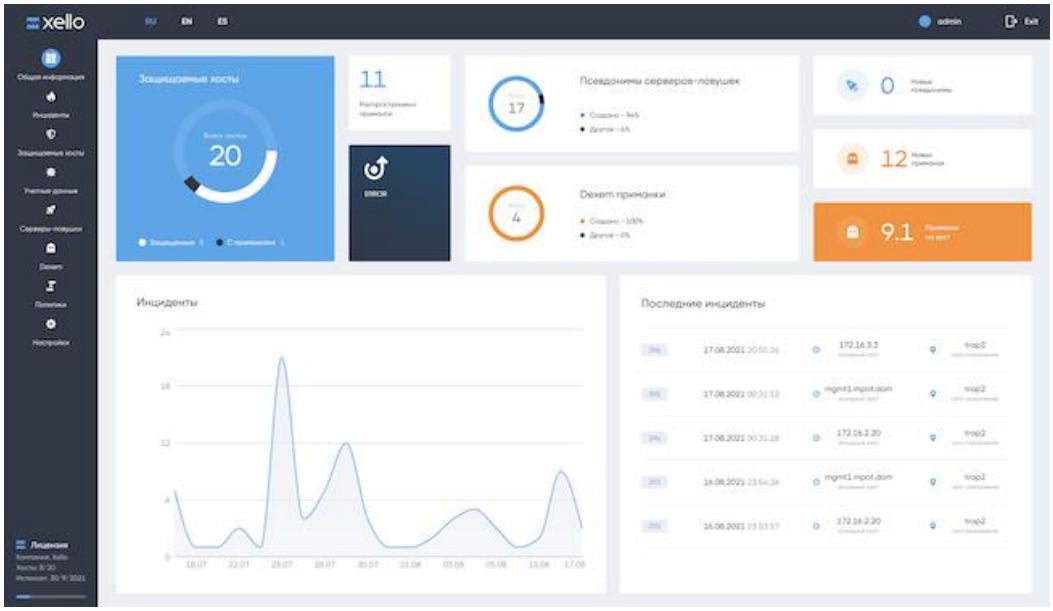

Рисунок 3.6. Основне меню Xello Deception

Пункт "Ліцензія" дозволяє завантажити ліцензію та отримати всі функціональні можливості Xello Deception. Після того, як ліцензію буде додано, продукт покаже всю необхідну інформацію про неї(Рисунок 3.7).

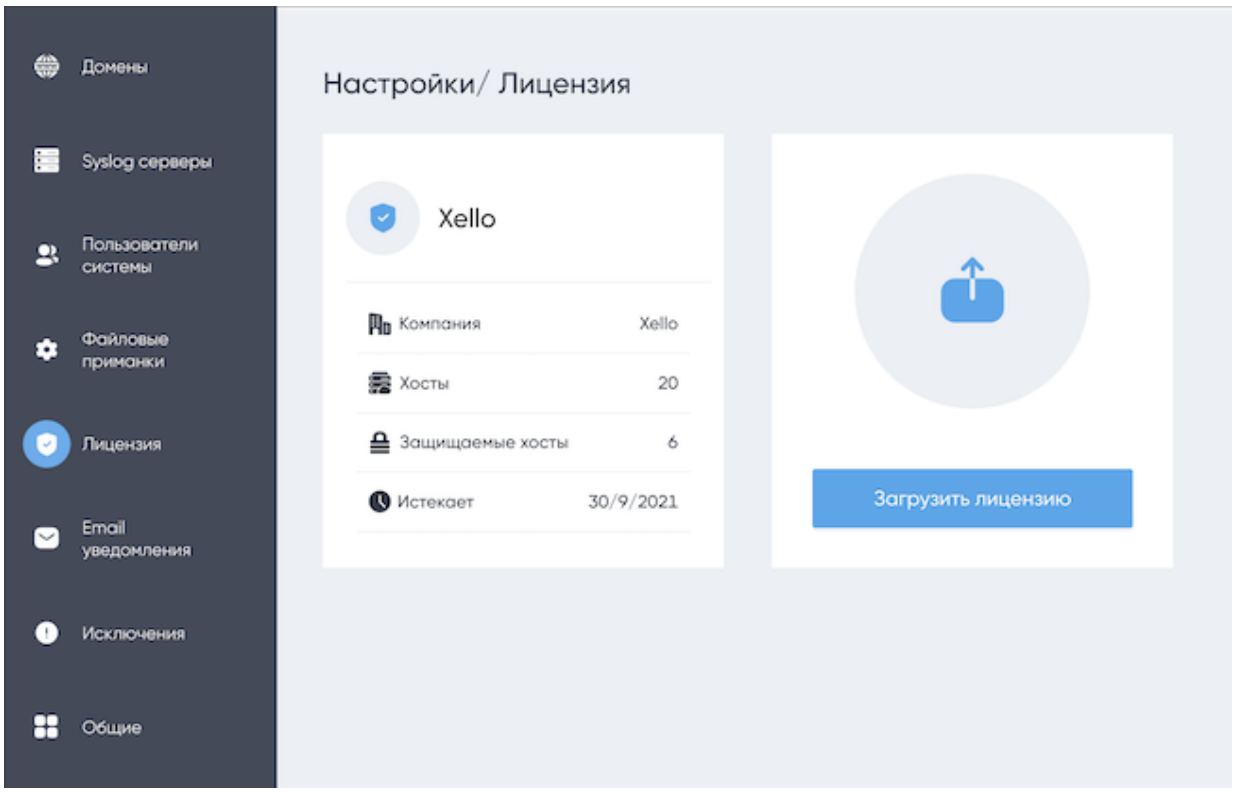

Рисунок 3.7. Додавання ліцензії до системи Xello Deception

У системі є інтеграція з доменами під керуванням Microsoft Active Directory. Для цього в пункті «Параметри» слід вибрати вкладку «Домени». Далі потрібно вказати найменування домену, з яким необхідно організувати взаємодію, та ідентифікатор NetBIOS, після чого натиснути кнопку «Додати».

Xello Deception забезпечує підтримку LDAPS. Для її підключення слід встановити прапорець "Використовувати LDAPS". Також тут можна вказати користувача розповсюдження та читання журналу AD (Рисунок 3.8).

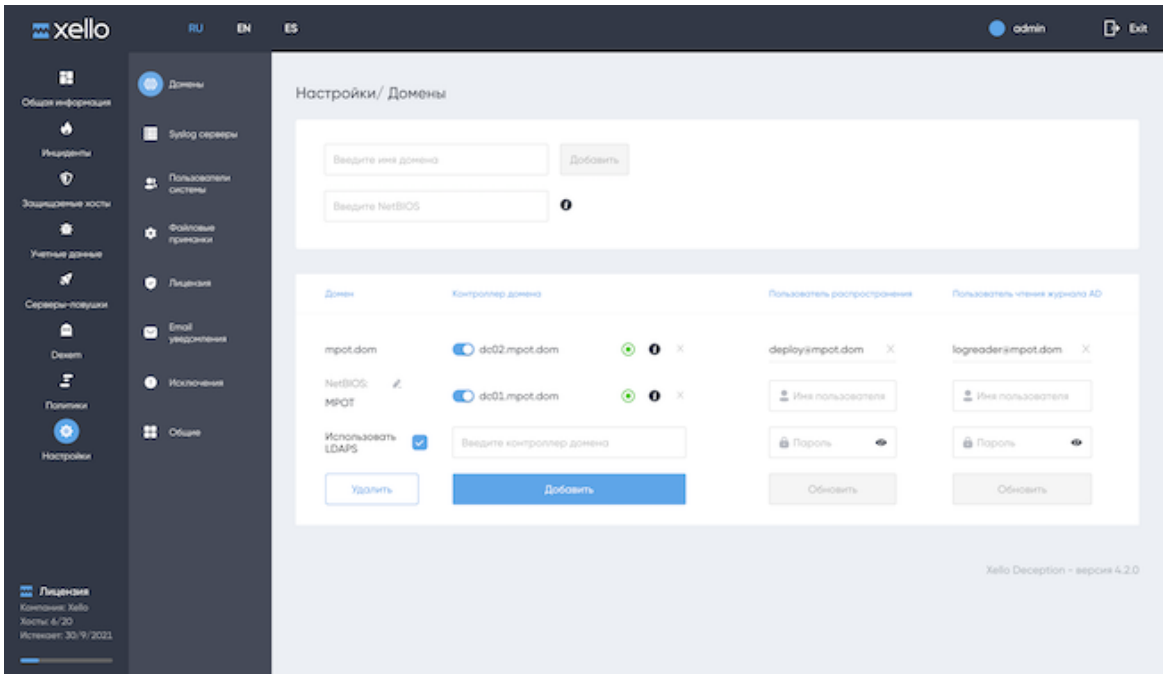

Рисунок 3.8. Підключення домену в Xello Deception

Керування користувачами реалізовано через вкладку «Користувачі системи» у розділі «Налаштування».

Створимо новий обліковий запис; Для цього необхідно вказати ім'я користувача, вибрати роль ("Admin", "Analyst", "Viewer") та натиснути на значок "+". У зв'язку з тим, що ми раніше підключали домен, необхідно вказувати назву цього домену. Також тут доступна зміна паролів адміністратора та сервісного користувача (необхідна для інтеграції з сервером-пасткою) (Рисунок 3.9).

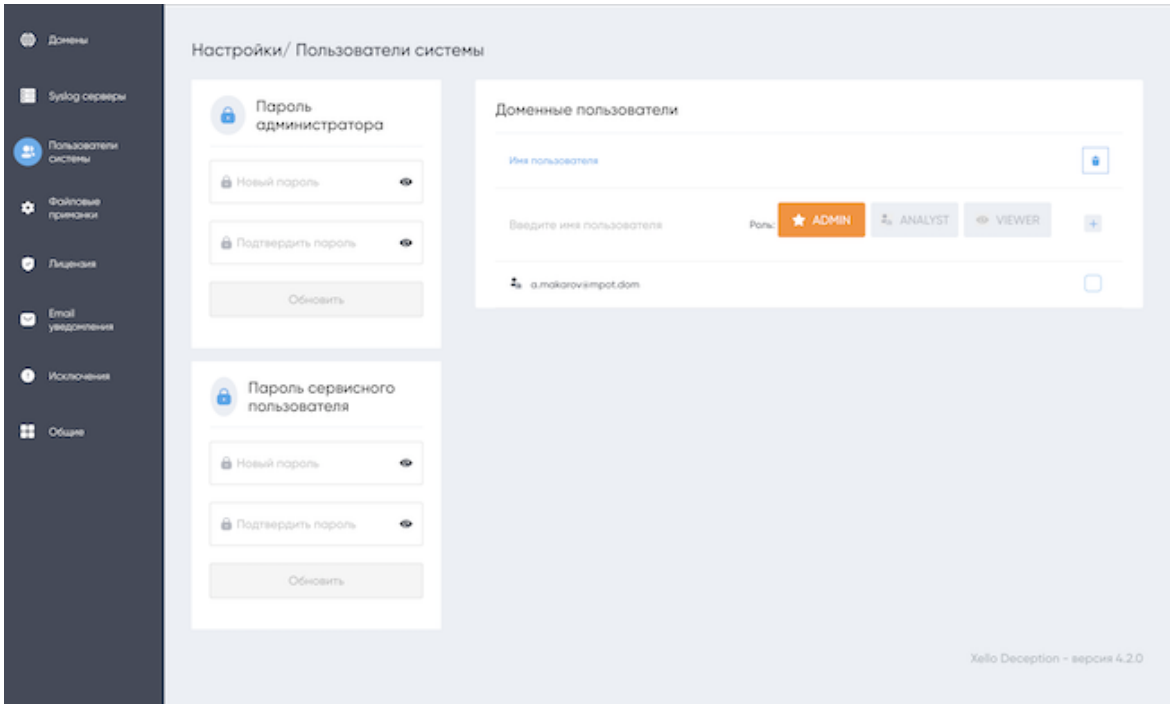

Рисунок 3.9. Додавання нового користувача до Xello Deception

Крім розглянутих вище опцій є ще вкладка «Загальні» (Рисунок 3.10). На ній є кілька дій. Наприклад, можна завантажувати архіви з журналами системи або звітами про інциденти в інформаційній безпеці, включати режим розширеного логування. Також вкладка дозволяє змінити деякі системні показники: видалити всі згенеровані облікові записи і додані приманки, привести стан системи до початкового (тобто зробити повне скидання до стану чистої установки), завершити всі активні сесії користувача, видалити інформацію по всіх інцидентах. Додатково можна завантажити скрипти розповсюдження та очищення для ОС Windows та Linux для їх подальшої ручної установки, наприклад за допомогою System Center Configuration Manager або Ansible.

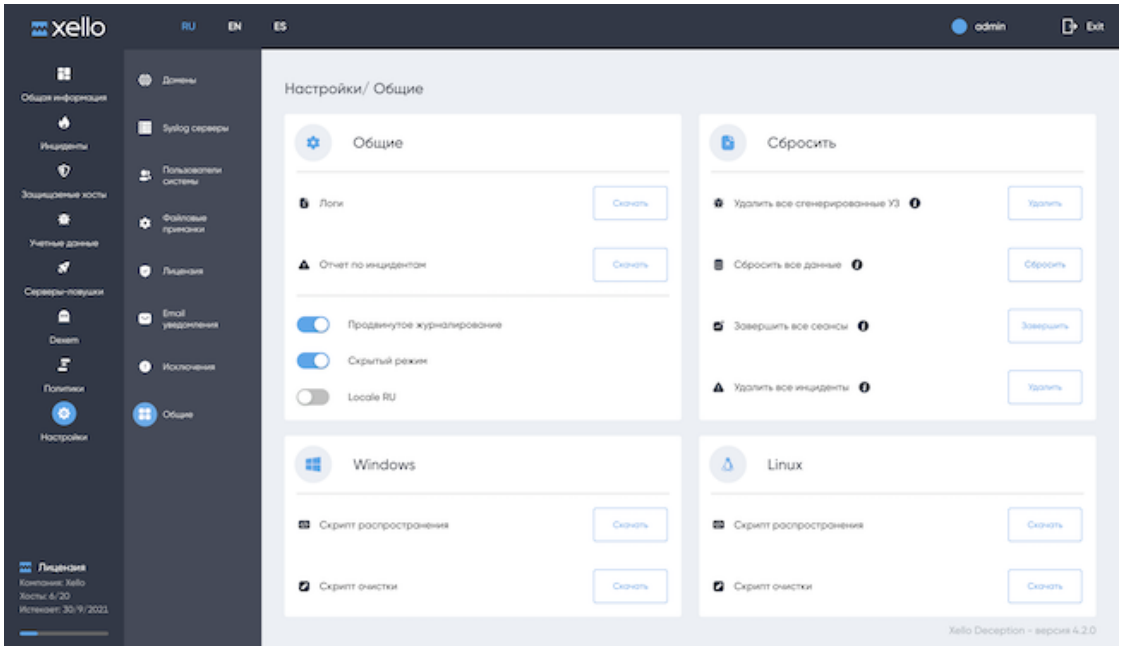

Рисунок 3.10. Огляд вкладки «Загальні» у Xello Deception

Вкладка «Винятки» (Рисунок 3.11) надає можливість керувати списками винятків для вихідних хостів, хостів призначення, користувачів та протоколів. Увімкнення створення інцидентів дозволяє створити конкретні сутностей та комплексні набори параметрів. Тільки при збігу всіх індикаторів подію буде проігноровано. Гнучка система правил дозволяє виключити будь-які хибно позитивні інциденти.

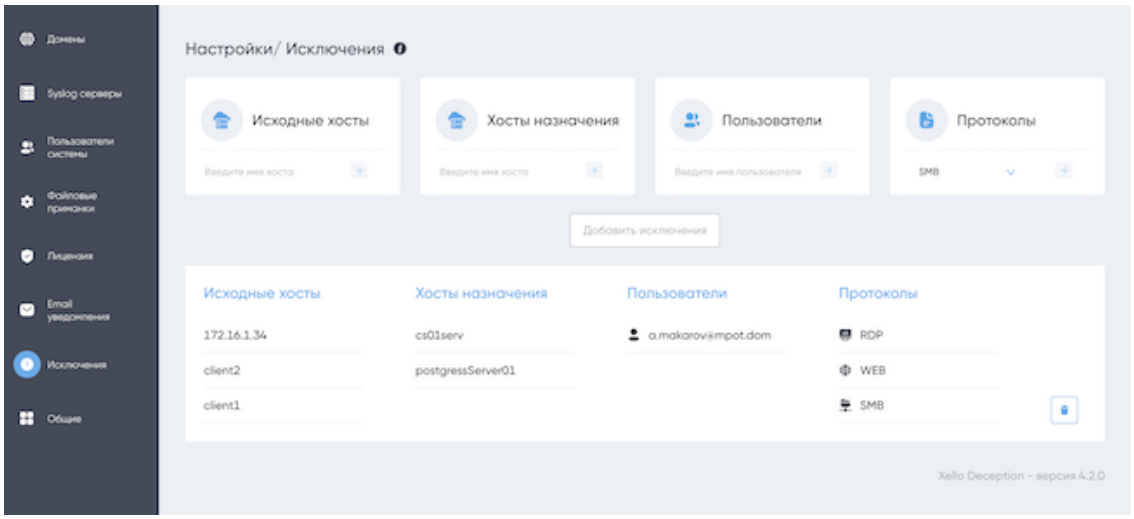

Рисунок 3.11. Додавання нових винятків у Xello Deception

Управління інформаційними повідомленнями реалізовано у підрозділі «Сповіщення» (Рисунок 3.12), де можна вказати поштовий сервер, через який

надсилатимуться поштові повідомлення, а також список електронних адрес їх одержувачів.

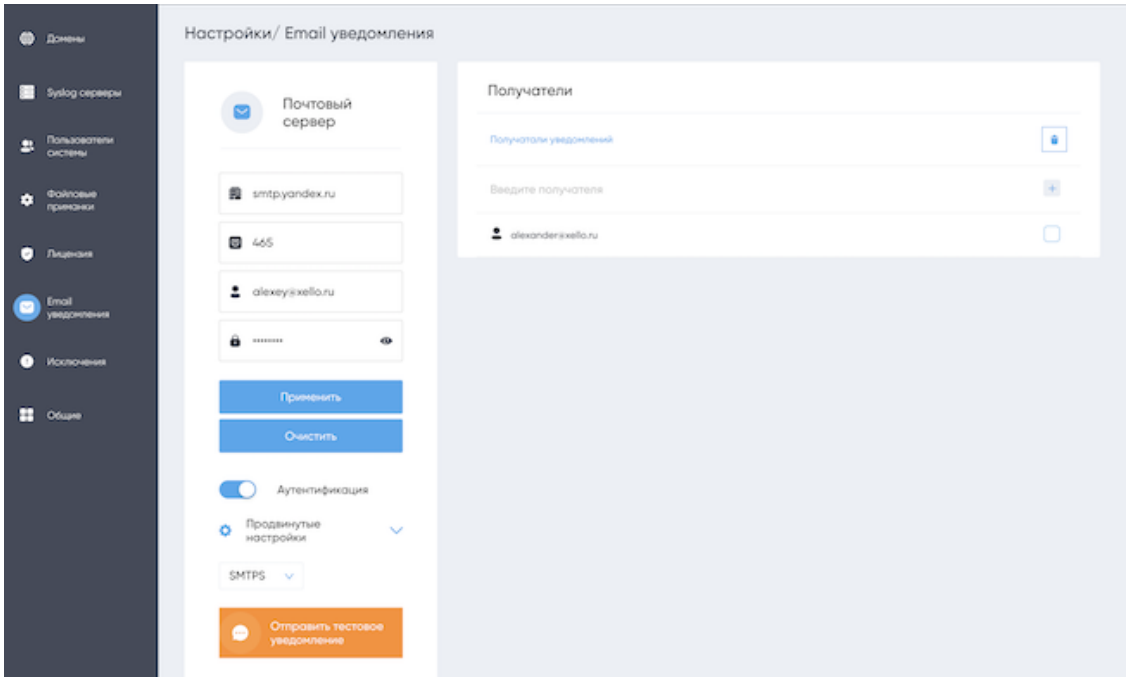

Рисунок 3.12. Налаштування повідомлень у Xello Deception

На вкладці «Syslog сервери» (Рисунок 3.13) можна додати нові або видалити старі сервери для збирання журналів даних. Щоб додати новий сервер, необхідно вказати ім'я хоста (наприклад, його IP-адресу), порт, протокол та формат передачі даних (CEF або JSON). У цьому пункті можна настроїти взаємодію з SIEM.

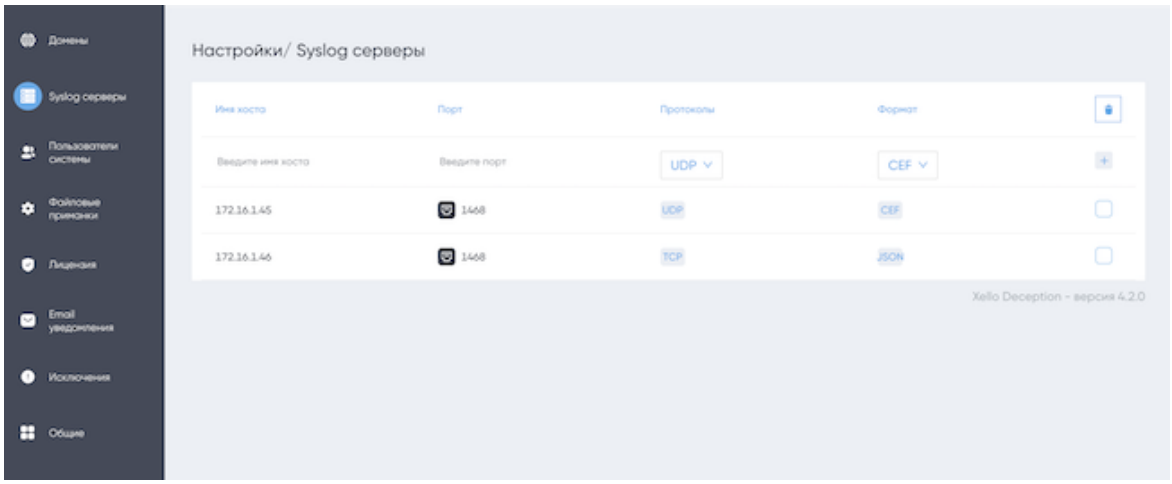

Рисунок 3.13. Управління Syslog-серверами у Xello Deception

Керування файлами приманок реалізовано через підрозділ "Файлові приманки" меню "Налаштування" (Рисунок 3.14). Доступно додавання нових приманок — для цього необхідно вказати шлях до заздалегідь створеного файлу з назвою, що привертає увагу, наприклад «psw.txt», а також доступне видалення непотрібних.

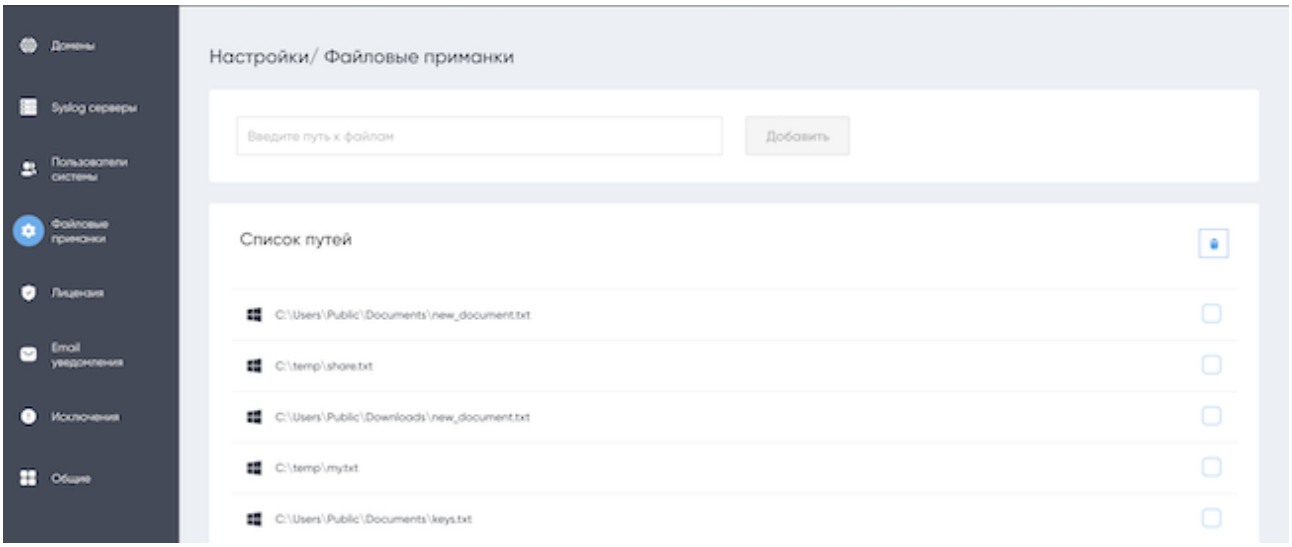

Рисунок 3.14. Зміна файлових приманок у Xello Deception

Усі основні відомості та віджети з поточними даними по системі розміщуються на вкладці «Загальна інформація» (Рисунок 3.15).

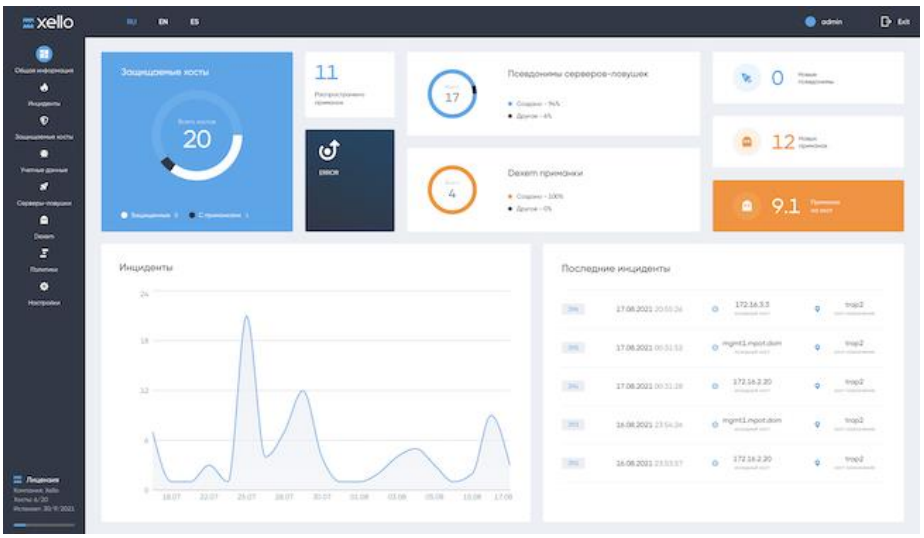

Рисунок 3.15. Перегляд даних на екрані із загальною інформацією у Xello Deceptio

Відображається кількість хостів, розповсюджених приманок, встановлених псевдонімів серверів-пасток і приманок створених з використанням технології Dexem. Також можна переглянути кількість інцидентів та відомості щодо останніх з них. Однак це вікно позбавлене інтерактивності, немає можливості перейти до потрібної вкладки при натисканні на ті чи інші дані. Також система не дозволяє настроювати параметри відображення даних.

3.5 Управління захищеними хостами у Xello Deception

Якщо відбувається інтеграція з Active Directory, в системі проводиться генерація набору пасток і приманок на основі облікових записів користувачів.

Управління цими елементами здійснюється на вкладках «Облікові дані» та «Сервери-пастки». На вкладці «Облікові дані» (Рисунок 3.16) міститься список облікових записів, які можуть бути приманками. Іншими словами, на основі реальних даних з Active Directory створюється список вигаданих користувачів з паролями, що легко підбираються. Також облікові записи користувачів можна створювати вручну; для цього необхідно ввести ім'я та пароль, а потім натиснути на значок "+".

Після того, як користувач з'явиться у списку, можна буде сформувати список протоколів для нього. Виходячи з того, які протоколи були обрані, приманки можуть бути наступними типами:

- Реквізити облікових записів у диспетчері облікових даних (Credential Manager).
- Кешовані маркери доступу до оперативної пам'яті.
- Збережені паролі у браузерах Chrome та Internet Explorer.
- Приманки з обліковими даними у вигляді файлів або скриптів PowerShell.
- Збережені SSH-ключі для доступу до віддалених серверів через WinSCP та Putty.
- Історія команд у bash.

- Збережені конфігурації та SSH-ключі AWS.
- Мережевий інтерфейс.

Після всіх цих процедур створений обліковий запис слід схвалити. Це робиться шляхом натискання на кнопку "Схвалити" навпроти імені користувача. Також можна схвалити всіх користувачів, натиснувши кнопку "Схвалити все". Користувачі поділяються на три категорії: Real (дійсні), Fake (створені методом адаптивної генерації Xello) і Disabled (відключені). Доступне сортування за цими параметрами.

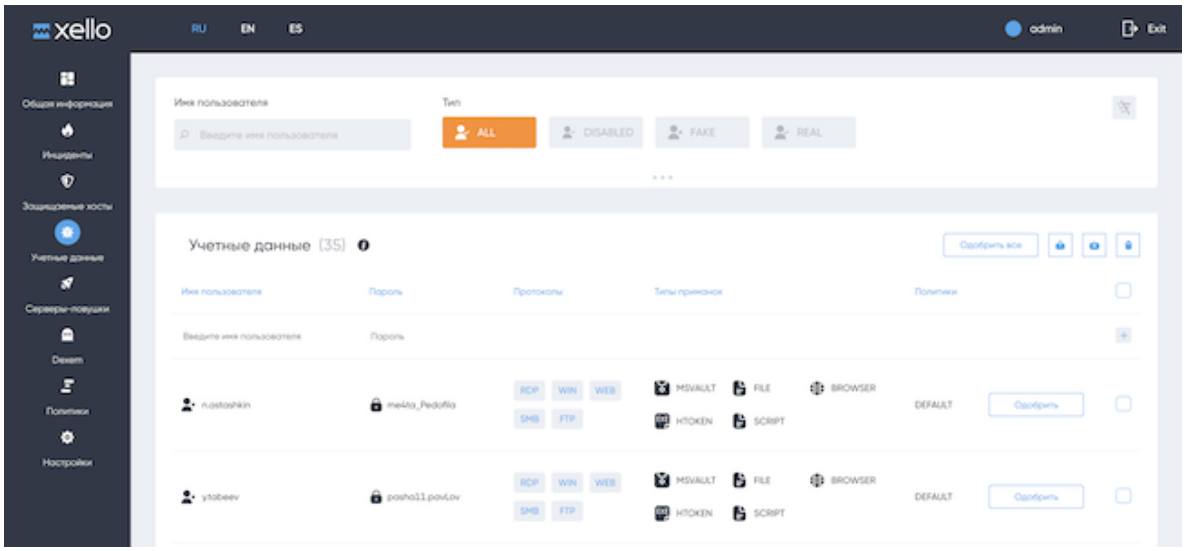

Рисунок 3.16. Створення нового користувача для приманки у Xello Deception

Завантаження даних про приманки можливе за допомогою імпорту файлів формату CSV з усіма обліковими даними; для цього потрібно натиснути на відповідну кнопку у правій частині вікна. Доступна й зворотна процедура – вивантаження всіх облікових записів користувачів із приманками у файл формату CSV. Управління приманками додатково реалізовано на вкладці «Сервери-пастки» (Рисунок 3.17). Загальний підхід до організації приманок чимось схожий на використовуваний у підрозділі «Облікові записи», але тут прив'язка йде не до облікових записів, а до DNS-імен або псевдонімів, які розміщуються на сервері-пастці. Крім того, тут представлений ширший перелік протоколів (SMB, RDP, WEB, SSH, ICMP, SCAN, FTP) та типів приманок (MSVAULT, WINSCP, PUTTY, FILE, BROWSER, SCRIPT). Ще однією

особливістю принад на основі псевдонімів є можливість створення декількох мережевих інтерфейсів, щоб розміщувати пастки у різних VLAN та підмережах. Щоб створити новий об'єкт, необхідно вказати DNS-запис, вибрати IP-адресу та натиснути на значок «+». Також тут можна вибрати IP-адресу з наявних мережевих інтерфейсів. Після цього знадобиться призначити типи протоколів, яких автоматично будуть прикріплені типи приманок, і натиснути кнопку «Схвалити». До цього об'єкта буде застосована політика встановлена за замовчуванням (default). Також можна завантажити та запустити скрипт на DNS-сервері, якщо він знаходиться під керуванням Windows Server. Це дозволить сформувати список об'єктів на DNS-сервері для створення оточення за технологією Deception.

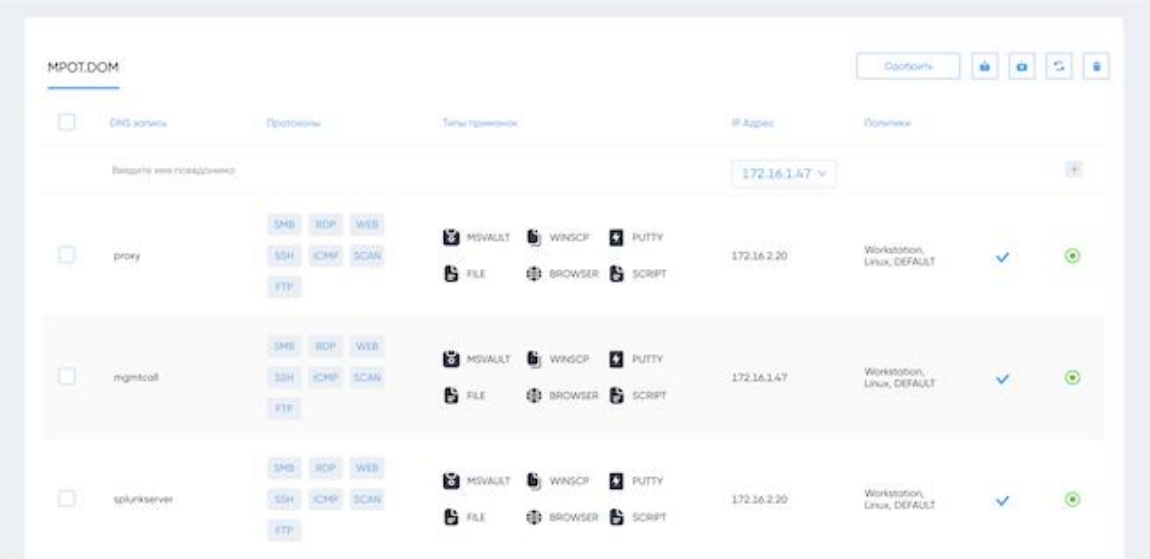

Рисунок 3.17. Розділ псевдонімів сервера-пастки у Xello Deception

Крім цього, на вкладці «Сервери-пастки» (Рисунок 3.18)можна керувати загальними папками, в яких розміщуватимуться приманки. Вони перебувають у полі "Папки спільного доступу". Доступні операції зі створення нових та видалення старих папок загального доступу. Папки створюються з цікавими для зловмисника назвами, наприклад, «licenses», «access» або «finance».

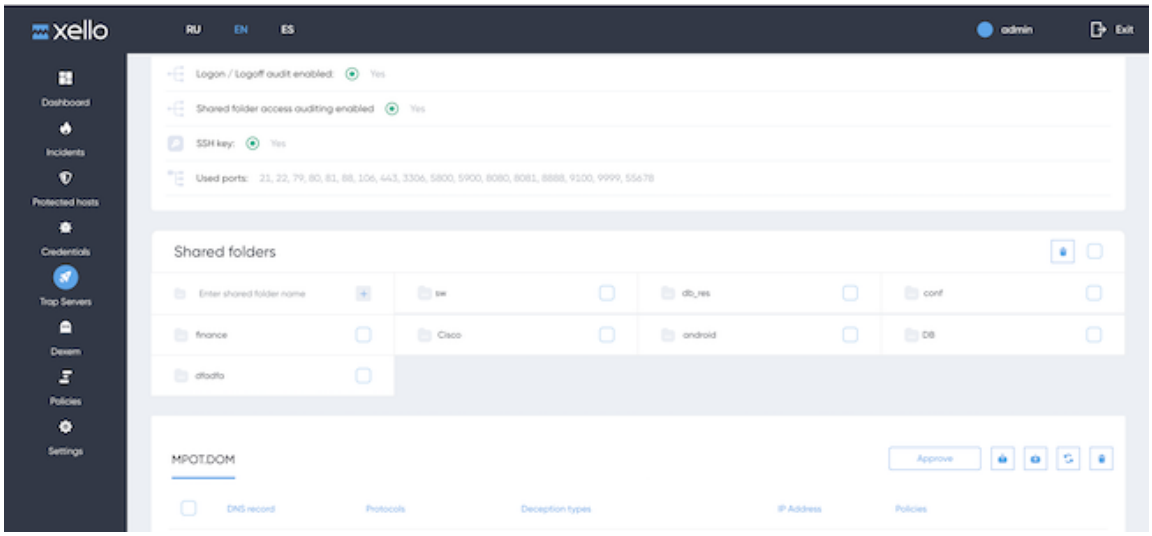

Рисунок 3.18. Керування папками спільного доступу до Xello Deception

Ще одним цікавим підрозділом є «Dexem» (Рисунок 3.19). Він служить для створення користувачів максимально схожих на реальних. Це запатентована технологія компанії Xello. Приманки створюються на основі даних з Active Directory. Відповідно, для того, щоб скористатися цією можливістю, необхідно заздалегідь провести інтеграцію з Active Directory і вказати дані домену через вкладку «Домени». Далі потрібно вибрати цільову групу користувачів Active Directory та ввести імена користувачів; всі необхідні атрибути для них буде створено автоматично. На наступному етапі за допомогою скрипта потрібно створити цих користувачів Active Directory. Далі система почне розповсюджувати ці облікові дані у вигляді приманок, які не відрізняються від реальних даних користувача.

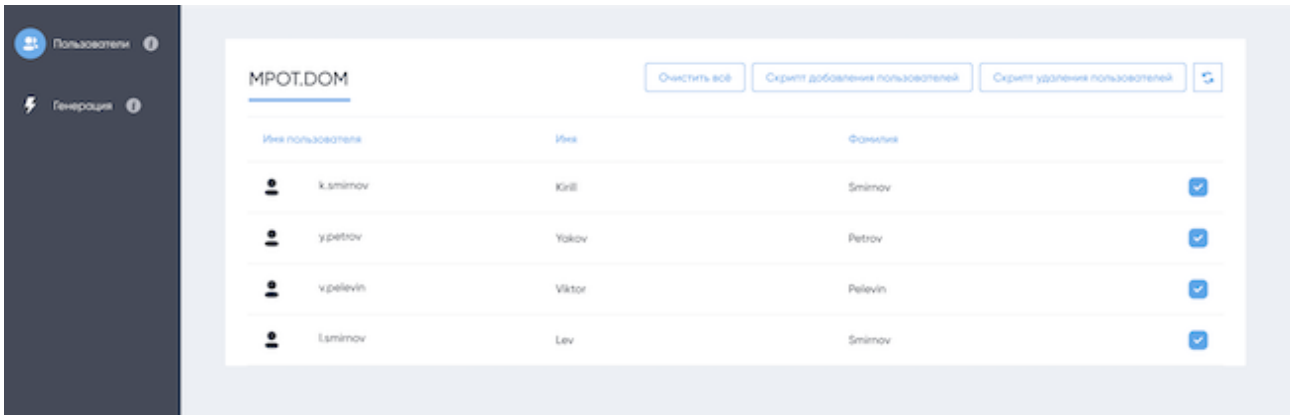

Рисунок 3.19. Генерація нових користувачів із застосуванням технології Dexem

Для створення приманок типу «Dexem» необхідно перейти на вкладку «Генерація», потім вибрати один із доступних доменів, який раніше був підключений. Далі у доступному вікні пошуку слід вибрати цільову групу користувачів та натиснути кнопку "Створити користувачів". Після цього буде згенеровано набір шаблонів з певним набором користувачів-приманок. Також для кожного шаблону необхідно ввести атрибути AD: «firstName», «lastName» та «userPrincipalName» (Рисунок 3.20). Після виконання всіх цих дій слід натиснути кнопку «Зберегти користувачів»; тоді приманки Dexem будуть додані до системи.

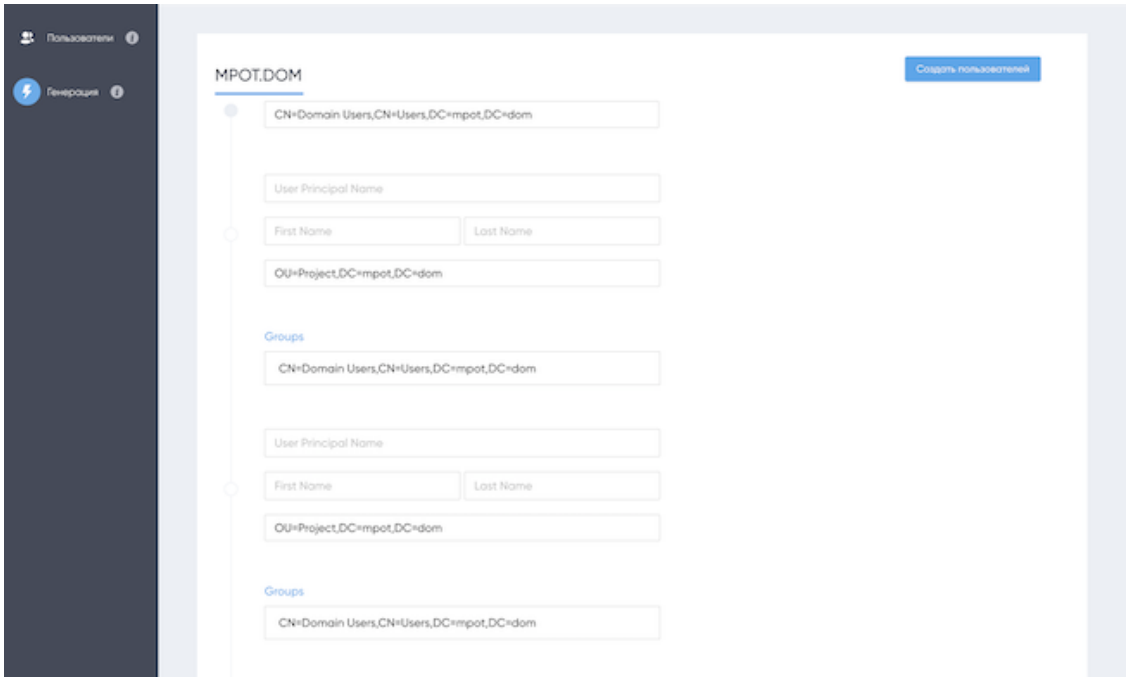

Рисунок 3.20. Створення користувача типу «Dexem» у Xello Deception

Управління хостами організації для розміщення на них приманок реалізовано через вкладку «Хости, що захищаються» (Рисунок 3.21). Тут у вигляді списку розміщено перелік вузлів, включаючи ім'я хоста, ім'я домену, захищені групи, політику, статус приманок і статус хоста. Також є сортування списку хостів за різними параметрами. Для фільтрації інформації про захищені хости необхідно натиснути на повзунок у верхній частині екрана. Після виконання цієї дії з'явиться панель фільтрів. Фільтрування доступне за такими категоріями: дата останнього розповсюдження приманки, статус

розповсюдження приманки, доступність хоста, ім'я домену, застосовувана політика , операційна система, відсоток встановлених принад.

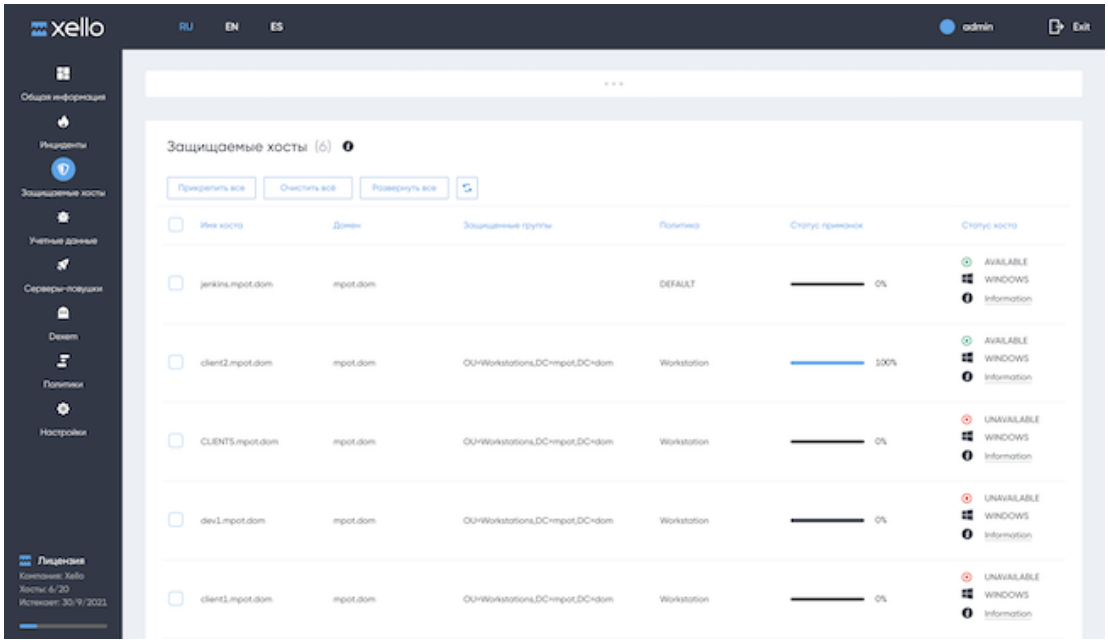

Рисунок 3.21. Розміщення приманок на хостах Xello Deception

У полі Статус хоста вказуються встановлена операційна система, доступність, а також дата і час розповсюдження приманки. Якщо натиснути на поле Статус принад, відкриється вікно, в якому можна побачити список всіх приманок, сформованих на основі псевдонімів (DNS-записів) та облікових записів користувачів із зазначенням протоколів та типів приманок. При натисканні на кнопку "Download" можна завантажити файл формату JSON з інформацією про приманки. Також поле "Статус приманок" показує відношення числа встановлених приманок до загальної кількості (у відсотках) (Рисунок 3.22).

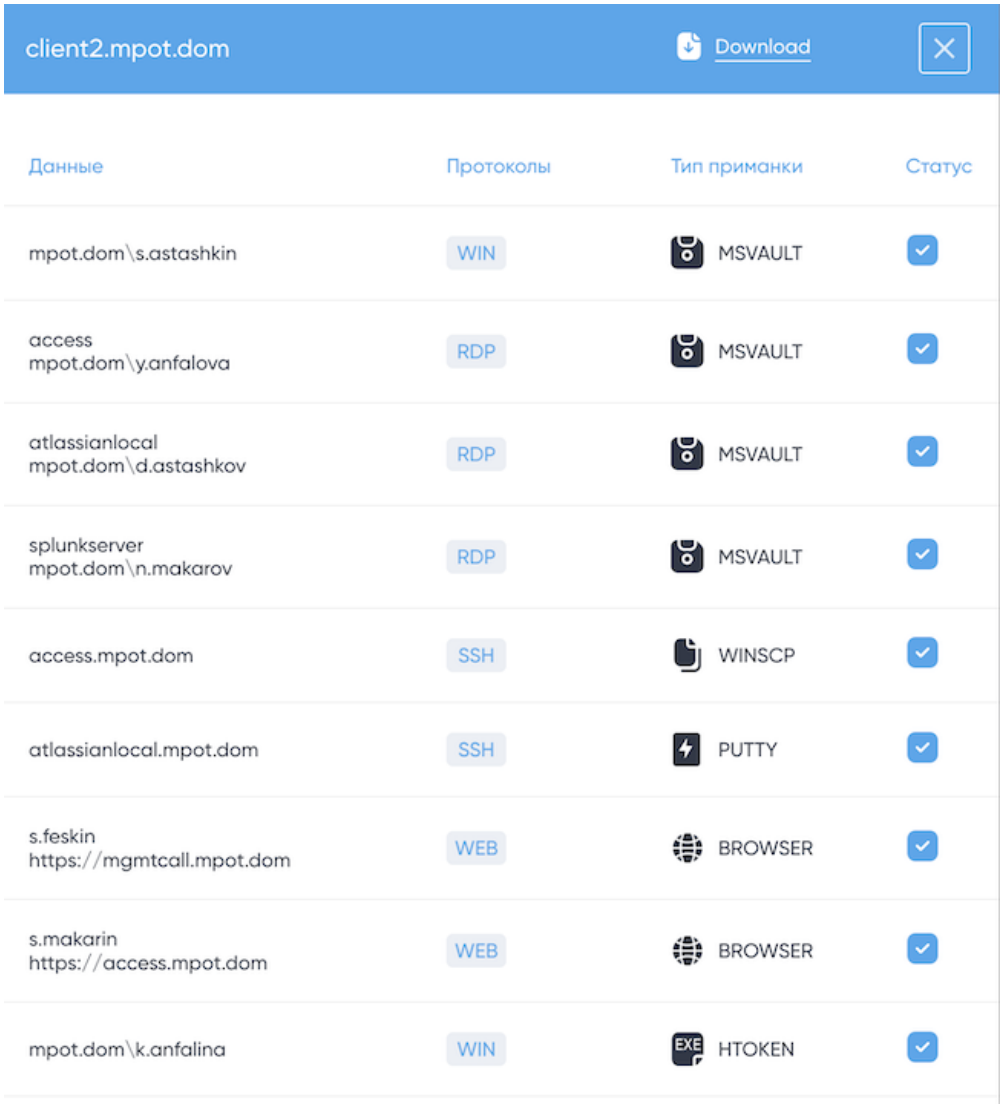

Рисунок 3.22. Перегляд списку приманок на хості

Крім того, в даному підрозділі можна поширити приманки на вибрані хости, що захищаються, перепризначити приманки або очистити хости, що захищаються, за допомогою відповідних кнопок.

3.6 Керування політиками в Xello Deception

Політики дозволяють об'єднувати набори хостів, що захищаються в групи, і налаштовувати для них правила захисту. У політику додаються захищені групи хостів, сервери-пастки та облікові дані приманок. Керування політиками здійснюється на вкладці "Політики" (Рисунок). Тут можна налаштовувати правила розповсюдження приманок для трьох груп об'єктів:

- облікові дані,

- псевдоніми серверів-пасток,
- захищені групи.

Кожна з них розміщується на окремій вкладці (Рисунок 3.23). Будь-який із елементів, представлених у цих групах, можна видалити. Для додавання нових облікових даних, псевдонімів чи груп необхідно скористатися кнопкою "+".

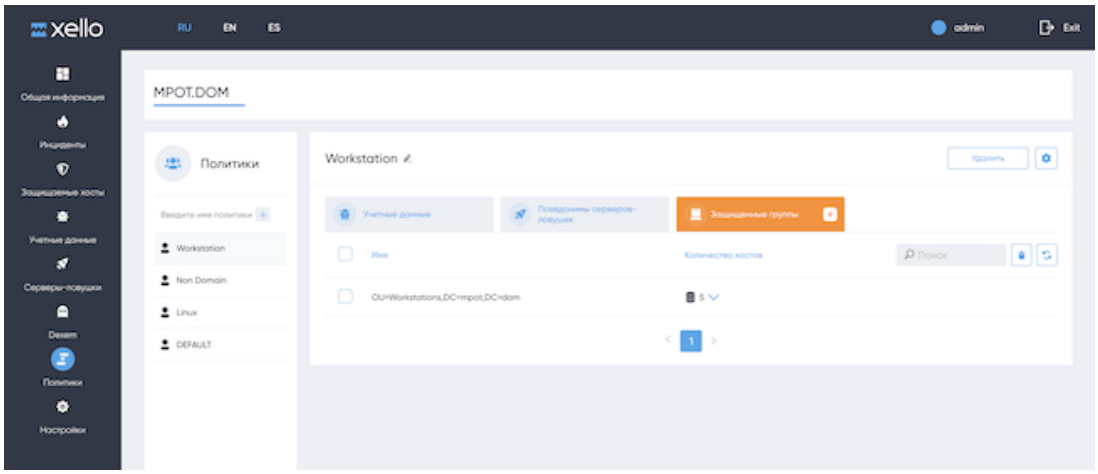

Рисунок 3.23. Управління правилами політик у Xello Deception

Наприклад, якщо додати нову групу до категорії «Захищені групи», з'явиться вікно, в якому можна вказати параметри додавання. Зокрема, можна вибрати хости тільки з певною операційною системою (родини Linux або Windows) або не в домені (Рисунок 3.24).

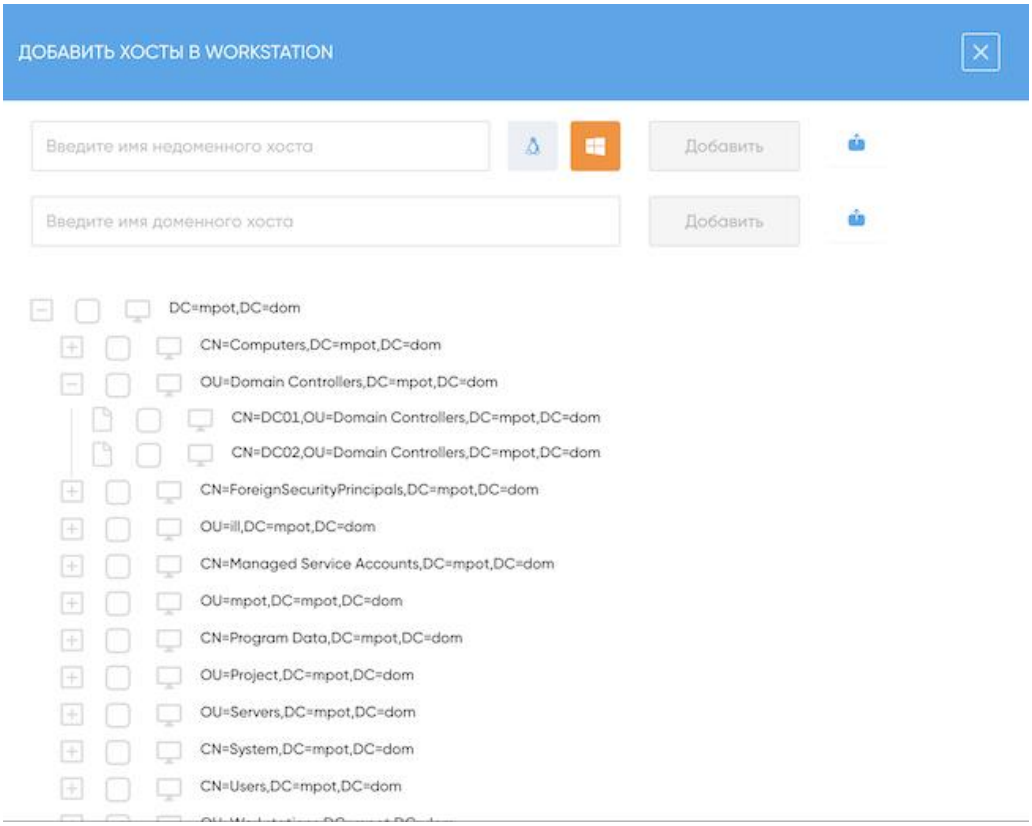

Рисунок 3.24. Додавання нової захищеної групи до Xello Deception

Також можна внести налаштування у вибрану політику, вказати кількість приманок, які поширюватимуться на хості. Опція «Розповсюдження за розкладом» (Рисунок 3.25) дозволить вказати час, в який розпочнеться встановлення приманок. Додатково можна вибрати використання технології Dexem та гостьового доступу для розкладання приманок у локальні профілі користувачів та на хости, що знаходяться не в домені. Реалізовано можливість вказати облікові записи користувачів для поширення приманок на хости під операційною системою Windows та/або Linux.

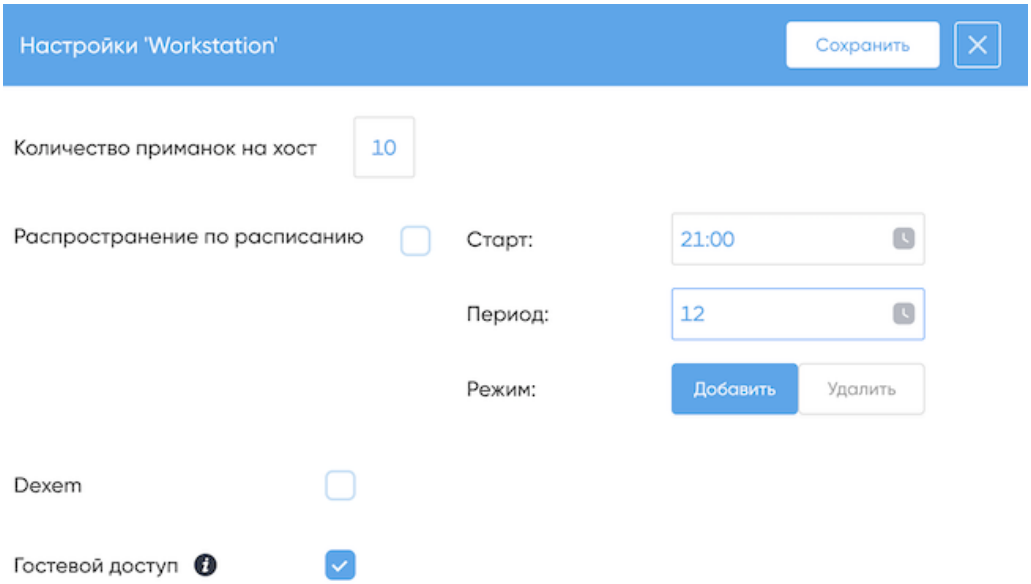

Рисунок 3.25. Внесення змін до налаштувань політики у Xello Deception

3.7 Управління інцидентами у Xello Deception

Управління інцидентами здійснюється за допомогою вкладки «Інциденти» (Рисунок 3.26). Усі інциденти розміщуються у вигляді списку та впорядковуються за часом та датою події. При цьому кожному інциденту надається свій ідентифікатор. Також можна з'ясувати, на якому захищеному хості стався інцидент, дізнатися про хост призначення (тобто ім'я сервера-пастки), протоколи, коментарі та статус інциденту (відкритий або закритий). Коментар можна додати під час обробки інциденту.

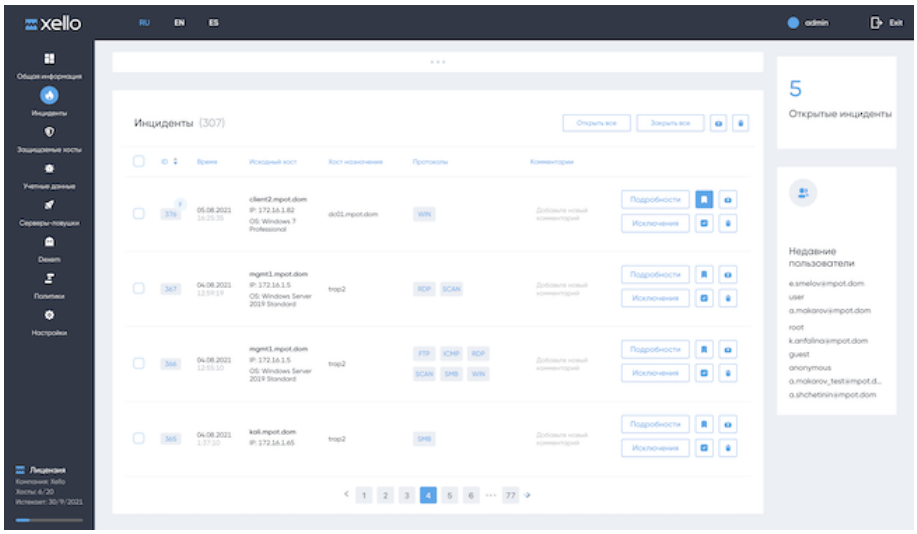

Рисунок 3.26. Перегляд інформації про інциденти у Xello Deception

Кожен інцидент може складатися як з однієї події, так і з кількох. Щоб побачити всі події з інциденту, необхідно перейти на сторінку, натиснувши на нього (Рисунок 3.27). У вікні буде інформація про хост — зокрема, категорія, доменне ім'я, встановлена ОС, IP-адреса та відкриті порти. Також можна з'ясувати, які дії ініціювали інцидент. У нашому прикладі було здійснено підключення за протоколом WEB до хосту. Можна подивитися інформацію про обліковий запис, за допомогою якого проводилося підключення, пароль і результат цих дій. Після того, як інцидент буде оброблений, його потрібно закрити, вказавши в коментарі, які дії були виконані, а також описавши особливості інциденту, наприклад уточнивши, що інцидент був хибно позитивним або проводилося тестування.

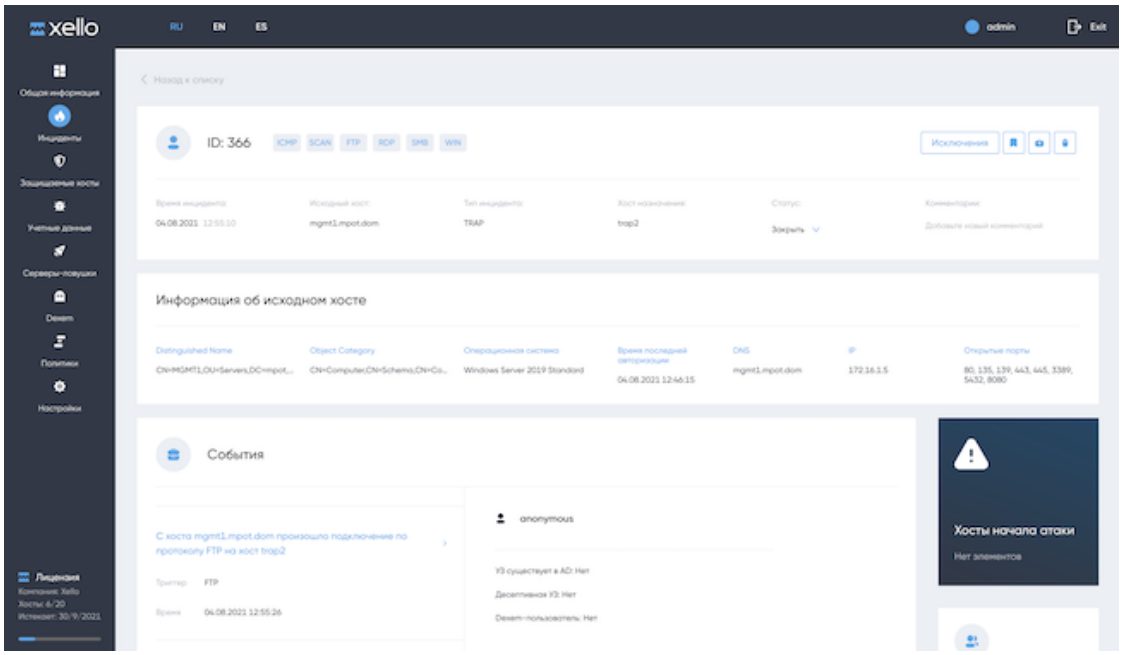

Рисунок 3.27. Перегляд докладнішої інформації про інцидент у Xello Deception

Також слід зазначити, що Xello Deception дозволяє збирати з атакованого хоста дані для проведення розслідування інциденту. Збір інформації відбувається автоматично. Для перегляду даних форензики необхідно натиснути на значок завантаження даних, а потім на рядок «Форензика» на вкладці «Інциденти» у рядку з інформацією про інцидент (Рисунок 3.28). Після цього слід натиснути кнопку «Download», щоб завантажити файл у форматі JSON. Також реалізовано можливість експорту даних про інциденти у файли формату

JSON та EXL. Ще однією особливістю вкладки «Інциденти» є можливість додавати складові інцидентів (наприклад, облікові дані користувачів, вихідний хост та хост призначення, протоколи) у виключення. Це робиться шляхом натискання на кнопку «Виключення» та вибору необхідних значень. Таким чином, можна, наприклад, прибрати помилкові спрацьовування під час тестування системи.

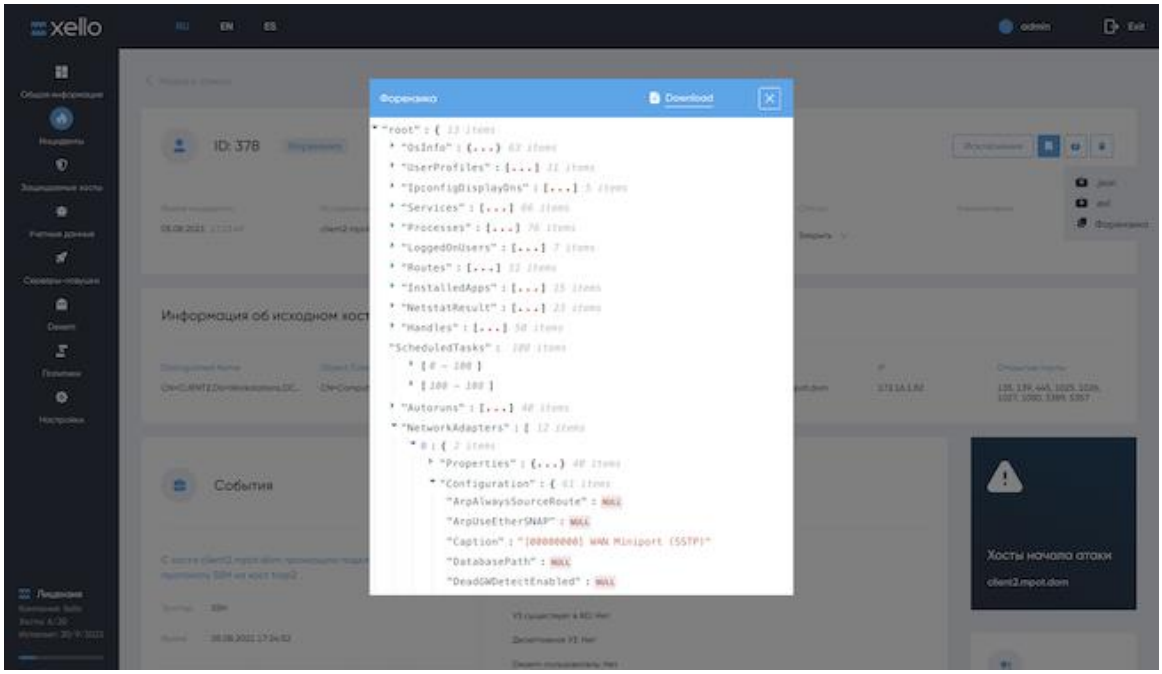

Рисунок 3.28. Завантаження даних форензики про інцидент у Xello Deception

3.8 Сценарій реагування на дії зловмисника

Розглянемо як через консоль адміністрування можна відстежити дії зловмисника, а саме — спробу проникнення в інфраструктуру. Для того щоб перевірити, як Xello Deception відреагує на атаку, спробуємо зімітувати активність кіберзлочинця. Запустимо на хості спеціальне програмне забезпечення для пошуку облікових записів та паролів (Рисунок 3.29).

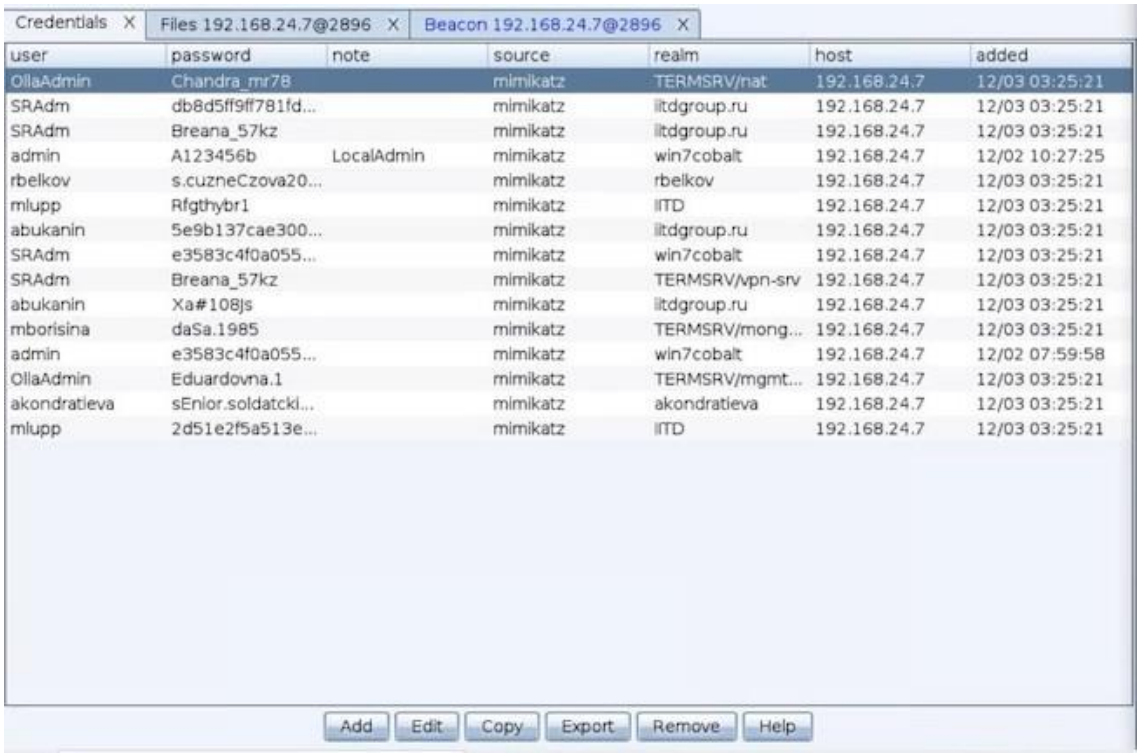

Рисунок 3.29. Пошук облікових записів та паролів в інфраструктурі

Як видно, нам вдалося отримати дані щодо різних облікових записів, у тому числі тих, хто має права адміністратора, а також паролі для кожного облікового запису. Далі намагаємося скористатися одним із вкрадених облікових записів з правами адміністратора для підключення до іншого хосту. Однак пароль виявляється невірним, і подальші спроби застосувати його також призводять до невдачі (Рисунок 3.30).

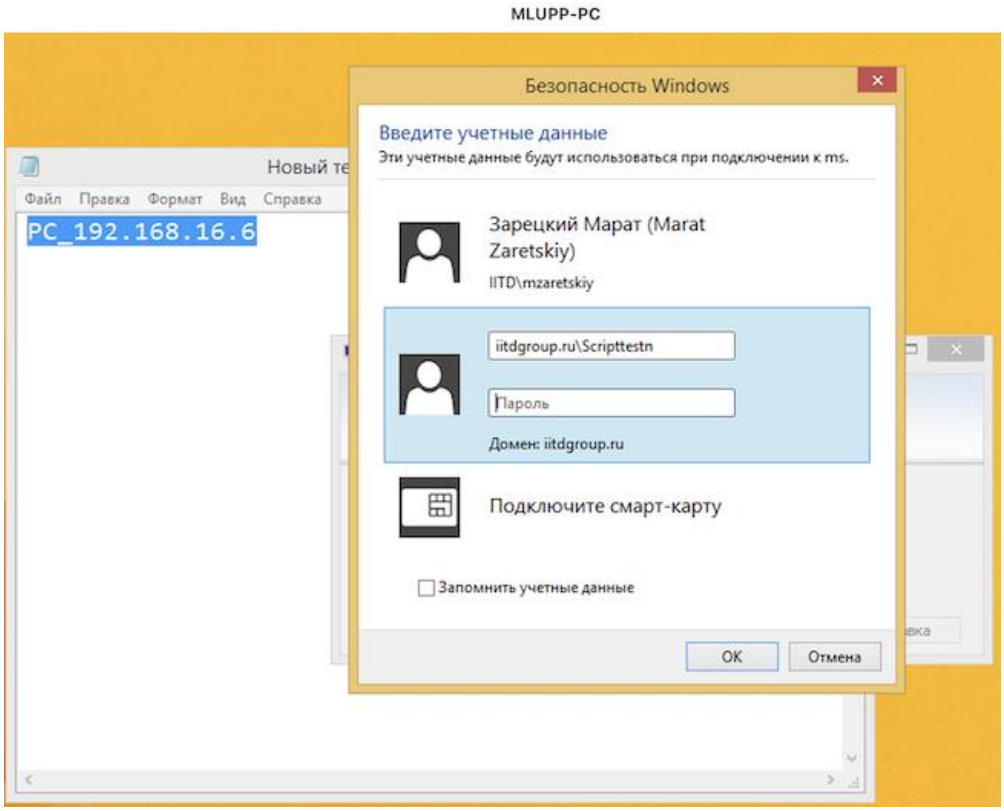

Рисунок 3.30. Спроба застосувати облікові дані для підключення до хосту

Усі ці дії Xello Deception фіксує як інцидент. Якщо зайти на вкладку «Інциденти», можна побачити події пов'язані з неуспішною авторизацією. Також показується тип приманки, який використали (Рисунок 3.31).

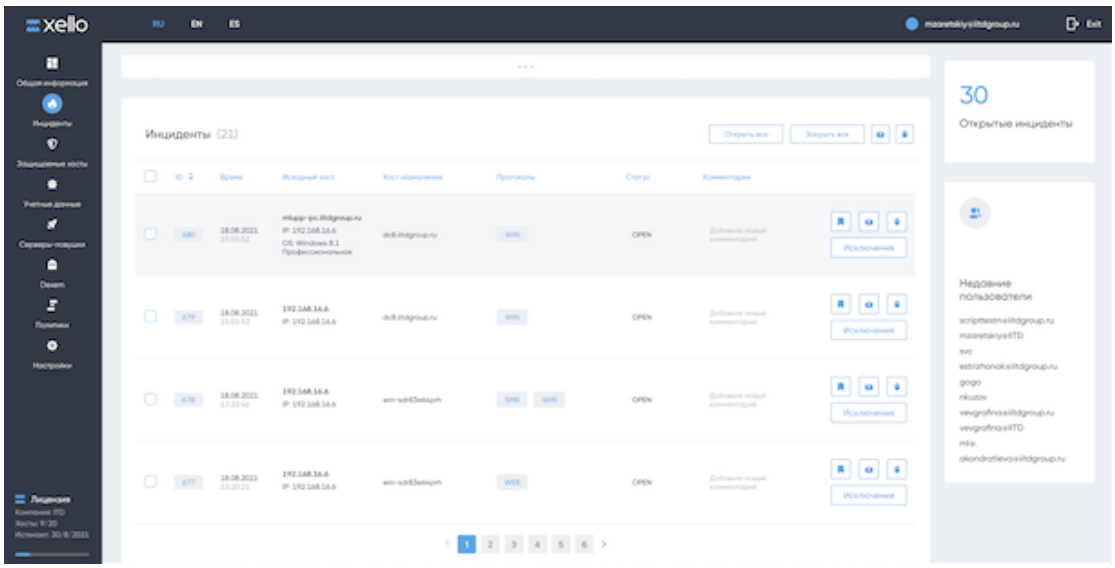

Рисунок 3.31. Список зафіксованих інцидентів у Xello Deception

Система захищає інфраструктури замовників від спрямованих атак, виявляючи та прогнозуючи дії зловмисників за допомогою приманок та пасток, що дозволяє оперативно підготуватися до подальших атак. Xello Deception пропонує централізоване та зручне керування принадами, забезпечує їх установку, а також дає можливість відстежувати інциденти через єдину консоль. При цьому пастки можуть встановлюватися на хости під керуванням як Windows, так і Linux. Також можлива інтеграція із системами класу SIEM, EDR, NAC, Sandbox. Ще однією особливістю є можливість роботи з форензикою для розслідування інцидентів, наприклад, силами аналітиків SOC. Не варто забувати, що «на борту» Xello Deception є запатентована технологія Dexem, яка дозволяє створювати помилкові облікові записи користувачів з максимально наближеними характеристиками до реальних, оскільки створюються вони на базі дійсних користувачів AD. Хочеться відзначити, що сегмент DDP надалі лише розвиватиметься, бо останнім часом намічається тенденція до збільшення кількості складних та цілеспрямованих атак.

ВИСНОВКИ

Організації повинні вважати, що зовнішні суб’єкти загроз або внутрішні зловмисники вже отримали доступ до систем і мереж або зроблять це в якийсь момент. Щоб захистити дані, вони повинні прийняти стратегію глибокого захисту, яка використовує різні методи та засоби контролю для запобігання, виявлення та реагування на атаки.

Технологія обману може бути широко розгорнута з впевненістю, що вона надасть кілька дуже цінних переваг:

- Проактивна позиція «припускати порушення» : розміщення технології обману на кінцевих точках, у Active Directory та в мережі припускає, що один із цих векторів атак із високим ризиком був, є чи буде зламаний.
- Зменшення втоми від сповіщень : лише суб’єкти загроз можуть викликати технологію обману для надсилання сповіщення, зменшуючи кількість помилкових спрацьовувань.
- Захист від «людського елемента», а саме зосередження на кінцевих цілях суб’єктів загрози спрямовано на їхню причину для участі в атаці, щоб пом’якшити людський елемент, який часто ігнорується в атаках.
- Розширити аналітику безпеки виявляючи лише зловмисні дії, групи безпеки можуть збагатити свої дані про загрози більш цілеспрямованими даними.
- Зменшення шуму оповіщення за допомогою технології обману означає, що групи безпеки можуть швидше реагувати на інциденти безпеки даних, покращуючи ключові показники, як-от середній час виявлення (MTTD), середній час на розслідування (MTTI) і середній час для реагування (MTTR).).
- Виявити інсайдерські загрози: підроблена інформація, яка використовується для захоплення зловмисників, також забезпечує видимість інсайдерів, які намагаються отримати доступ до ресурсів, які не є їх посадовою інструкцією.

Розуміння того, що таке технологія обману та переваги, які вона надає, може дати організаціям спосіб покращити свою позицію безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Achalvio T. Deception 2.0 / Team Achalvio., 2017. – 69 с.

2. Gartner [Електронний ресурс] – Режим доступу до ресурсу: https://www.gartner.com/en/publications/product-managers-top-priorities-for-tech-service-providers-leadership-vision-2021.

3. Лукацкий А. Обнаружение атак. — СПб.: БХВ-Петербург, 2001. – 624 с

4. Технологии обнаружения вторжений [Електро-нний ресурс] Режим доступу https://www.bytemag.ru/articles/detail.php?ID=6850&sphrase_id=3833171

5. Системи управління, навігації та зв'язку. – 2017. – №3. – С. 57–62.

6. Карачка А. Ф. ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ / А. Ф. Карачка. – Тернопіль, 2017. – 86 с.

7. Send attackers on a wild goose chase with deception technologies [Електронний ресурс]. – 2015. – Режим доступу до ресурсу: https://www.csoonline.com/article/2956573/send-attackers-on-a-wild-goose-chase-with-deception-technologies.html.

8. Технология обмана. Что такое Deception и как теперь обманывают хакеров [Електронний ресурс] // xakep. – 2020. – Режим доступу до ресурсу: https://xakep.ru/2020/07/28/deception/.

9. Joshi R. C. Honeypots A New Paradigm to Information Security / R. C. Joshi, A. Sardana., 2011. – 339 с. – (Science Publishers).

10. Mohssen M. Honeypots and Routers Collecting Internet Attacks / M. Mohssen, R. Habib-ur., 2016. – 192 с. – (Taylor & Francis Group).

11. deception technology [Електронний ресурс] – Режим доступу до ресурсу: https://whatis.techtarget.com/definition/deception-technology.

12. Mitnick K. The art of Deception / K. Mitnick, W. Simon.. – 577 с.

13. Acalvio ShadowPlex Autonomous Deception [Електронний ресурс] – Режим доступу до ресурсу: https://www.acalvio.com/product/.

14. Attivo ThreatDefend for ICS Systems [Електронний ресурс] – Режим доступу до ресурсу: https://cybersecurity-excellence-awards.com/candidates/attivo-threatdefend-for-ics-systems-2/.

15. Attivo Networks® Awarded U.S. Department of Defense Contracts for Active Cyber Defense and Cyber Deception Technology [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.businesswire.com/news/home/20210715005246/en/Attivo-Networks%C2%AE-Awarded-U.S.-Department-of-Defense-Contracts-for-Active-Cyber-Defense-and-Cyber-Deception-Technology.

16. Lure Attackers Away from Assets with Deception Technology [Електронний ресурс] – Режим доступу до ресурсу: https://fidelissecurity.com/platforms/fidelis-deception/.

17. Обман злоумышленников с помощью ловушек TrapX DeceptionGrid Источник: https://www.anti-malware.ru/practice/methods/TrapX-DeceptionGrid [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://www.anti-malware.ru/practice/methods/TrapX-DeceptionGrid.

18. ThreatDefend® Detection & Response Platform [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.attivonetworks.com/product/threatdefend/.

19. Xello Deception [Електронний ресурс] – Режим доступу до ресурсу: https://www.dialognauka.ru/products/Xello_Deception/.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ
(Презентація)