LABYRINTH

Labyrinth Deception Platform

Унікальний рівень розуміння безпеки

Сучасний стан інформаційної безпеки

Кібератаки продовжують ставати більш вдосконаленими та витонченими. У 2019 році malware-free атаки становили 51% всіх виявлених спроб вторгнення в інформаційні системи.

Фаєрволів та антивірусів недостатньо, щоб зупинити зломи та захистити ваші конфіденційні дані. Не існує Prevention інструментів, які могли б гарантувати 100% захисте від витоку інформації.

Більш ефективні рішення для виявлення кіберзагроз вимагають інфраструктури, якою потрібно керувати, і генерують величезну кількість оповіщень, які потрібно обробляти та інцидентів, які потребують розслідування кваліфікованим персоналом.

Сучасний стан інформаційної безпеки

Сучасні методи та техніки виявлення кібер загроз здебільшого грунтуються на роботі з Big Data.

SIEM, UEBA, EDR та інші рішення збирають якомога більше даних та проводять їх аналіз для виявлення потенційних загроз.

Цей підхід ефективний, але вимагає забагато ресурсів.

Проблеми використання Big Data

ПРОБЛЕМА КІЛЬКОСТІ

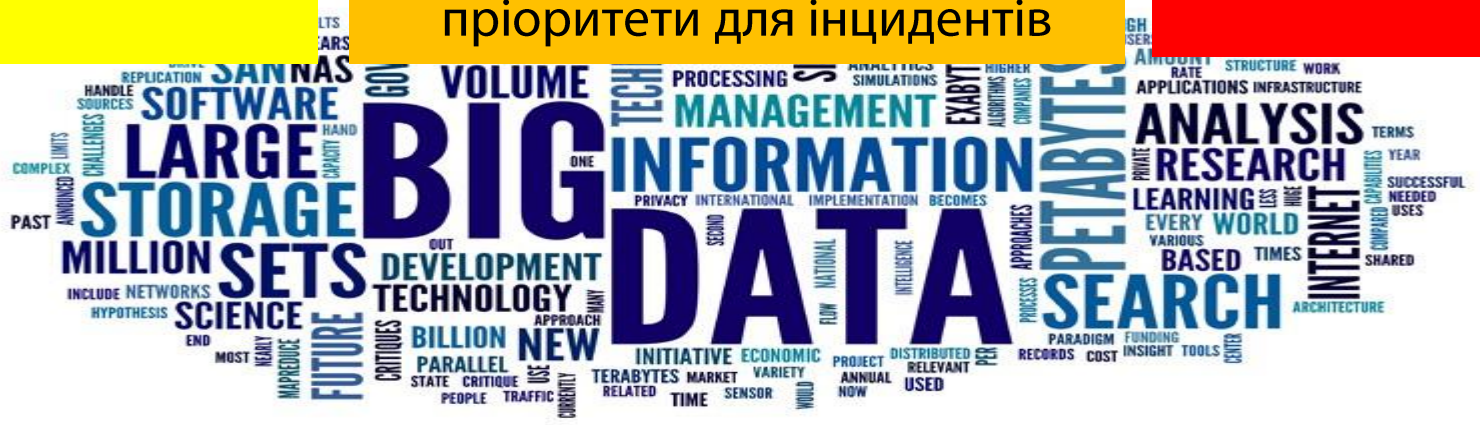
- високі витрати на централізацію логів та метадати
- дані займають багато місця при зберіганні
- аналітика даних вимагає багато обчислювальних ресурсів

ПРОБЛЕМА ОБРОБКИ

- надмірна кількість сповіщень, які потребують обробки
- високий показник помилково-позитивних сповіщень
- неможливість розставити пріоритети для інцидентів

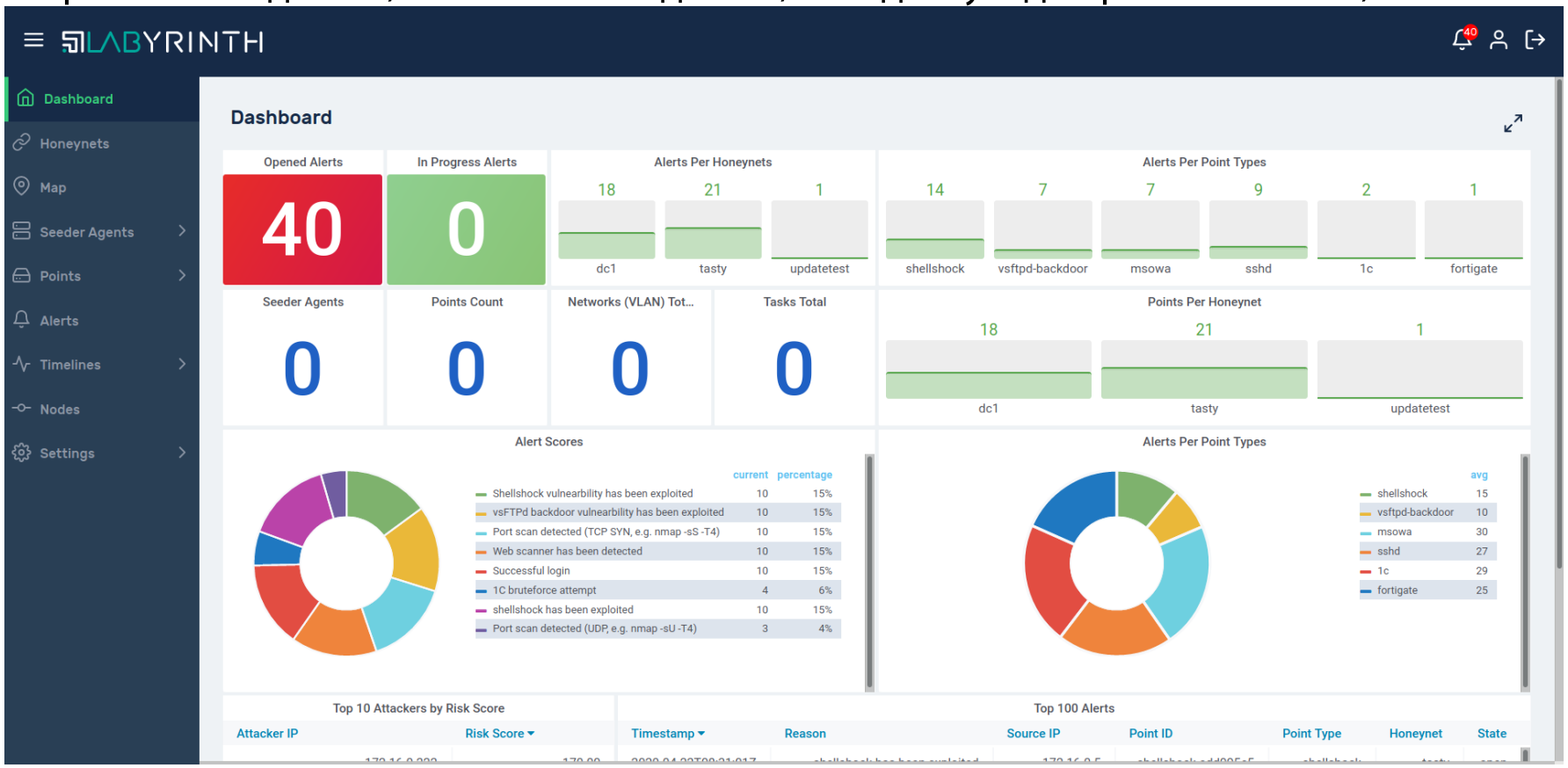
ПРОБЛЕМА ЕКСПЕРТИЗИ

- відсутність кваліфікованого персоналу
- висока вартість навченого персоналу
- неадекватна реакція на інциденти



Labyrinth Deception Platform

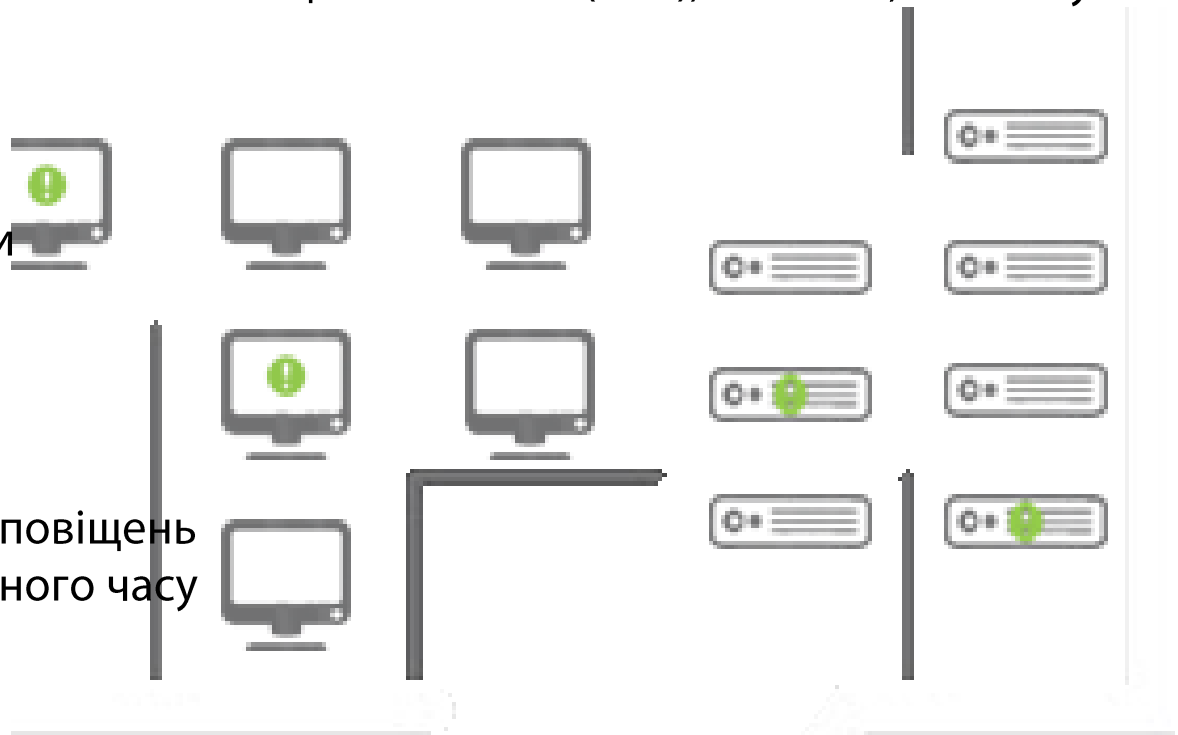
Labyrinth Deception Platform змінює парадигму кібербезпеки, підходячи до виявлення загроз як до проблеми "правильних даних", а не "великих даних", на відміну від виробників SIEM, UEBA або EDR.



Платформа надає атакуючим ілюзію вразливостей IT сервісів та додатків. Labyrinth провокує зловмисників на дії, виявляє та відстежує всю їхню діяльність та ізолює їх від реальної IT-мережі.

Labyrinth Deception Platform

Labyrinth Deception Platform допомагає ефективно протидіяти найбільш складним кібер загрозам. Функціонал рішення надає потужніші можливості для виявлення цільових атак (APT), ботнетів, zero-day та malware-free атак.

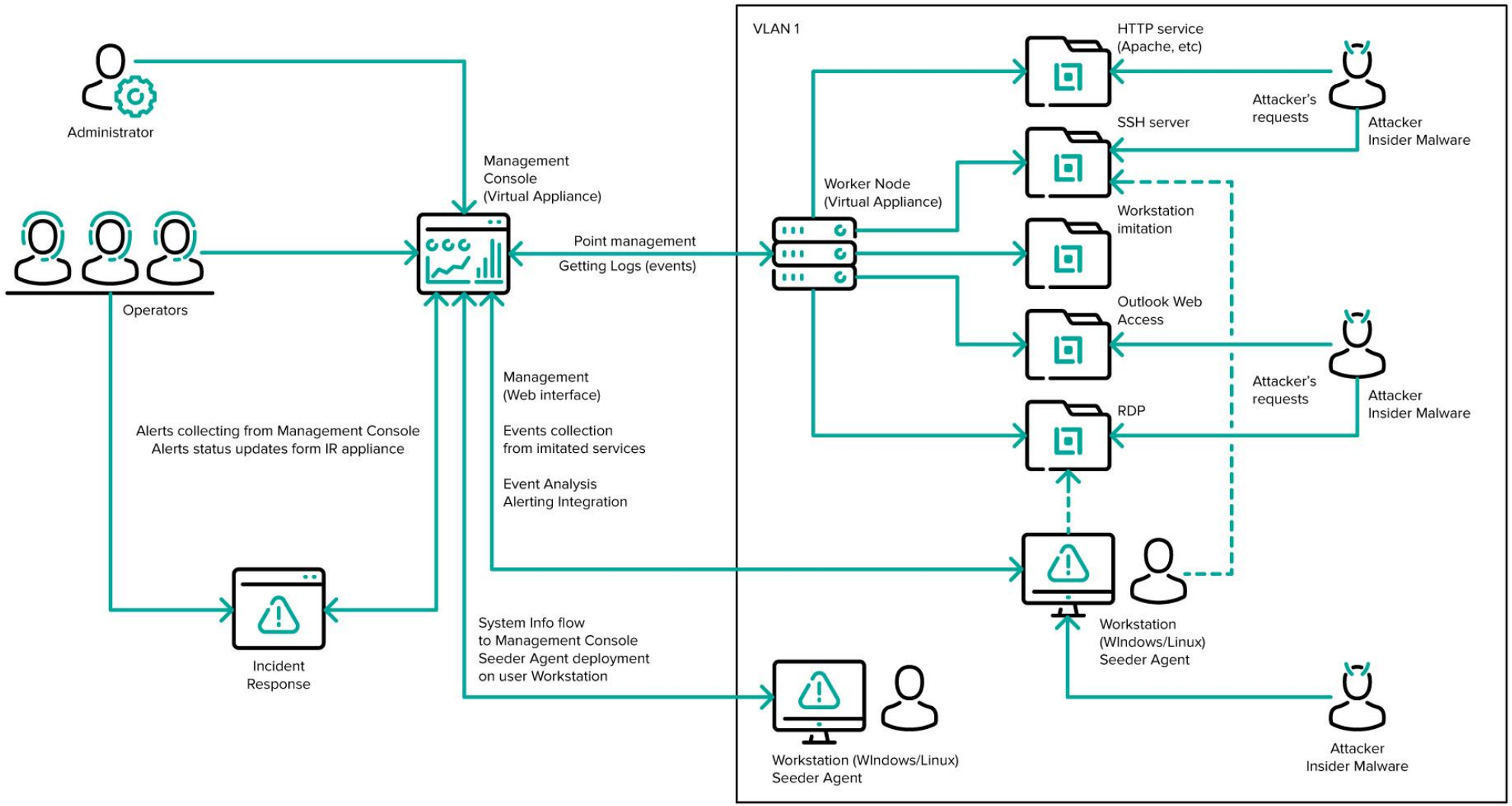


Немає проблеми з кількістю даних
- Не потребує збору величезної кількості даних
- Збирає лише дані, пов'язані з інцидентами безпеки
- Нульовий вплив на продуктивність IT мережі

Немає проблеми обробки даних
- Не генерує "цифровий шум"
- Вкрай низький показник помилково позитивних сповіщень
- Забезпечує повну видимість атаки в режимі реального часу

Немає проблеми експертизи
- Проста установка та конфігурація
- Ніяких спеціальних навичок для користування рішенням
- Автоматизоване виявлення та реагування

Архітектура рішення



Архітектура рішення

Seeder агенти працюють на серверах та робочих станціях, імітуючи привабливі артефакти. При спрацюванні агент спрямовує зловмисників до Point.

Робоча нода є хостом для всіх Point у Labyrinth. Вона працює в декількох VLAN одночасно.

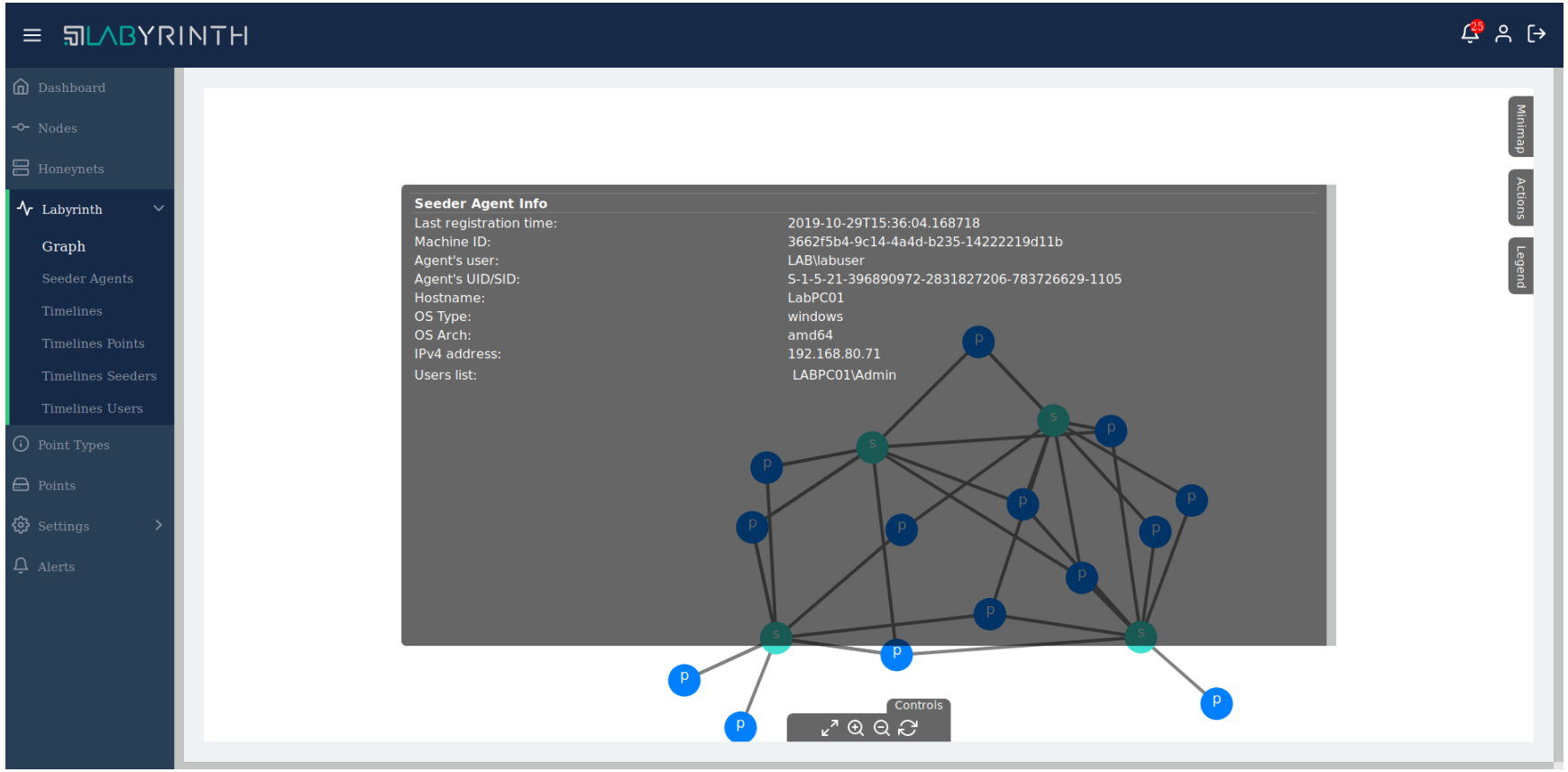
Point імітує вміст та сервіси, що відповідають його мережевому оточенню, та утримує зловмисників у Labyrinth, поки не буде зібрана вся необхідна інформація.

Вся зібрана інформація надходить на консоль управління для аналізу. Консоль надсилає необхідні дані на платформу реагування на інциденти.

IR перевіряє метадані в зовнішніх базах даних та прискорює реагування на інциденти за допомогою сторонніх інтеграцій, які автоматизують ізоляцію, блокування та пошук загроз.

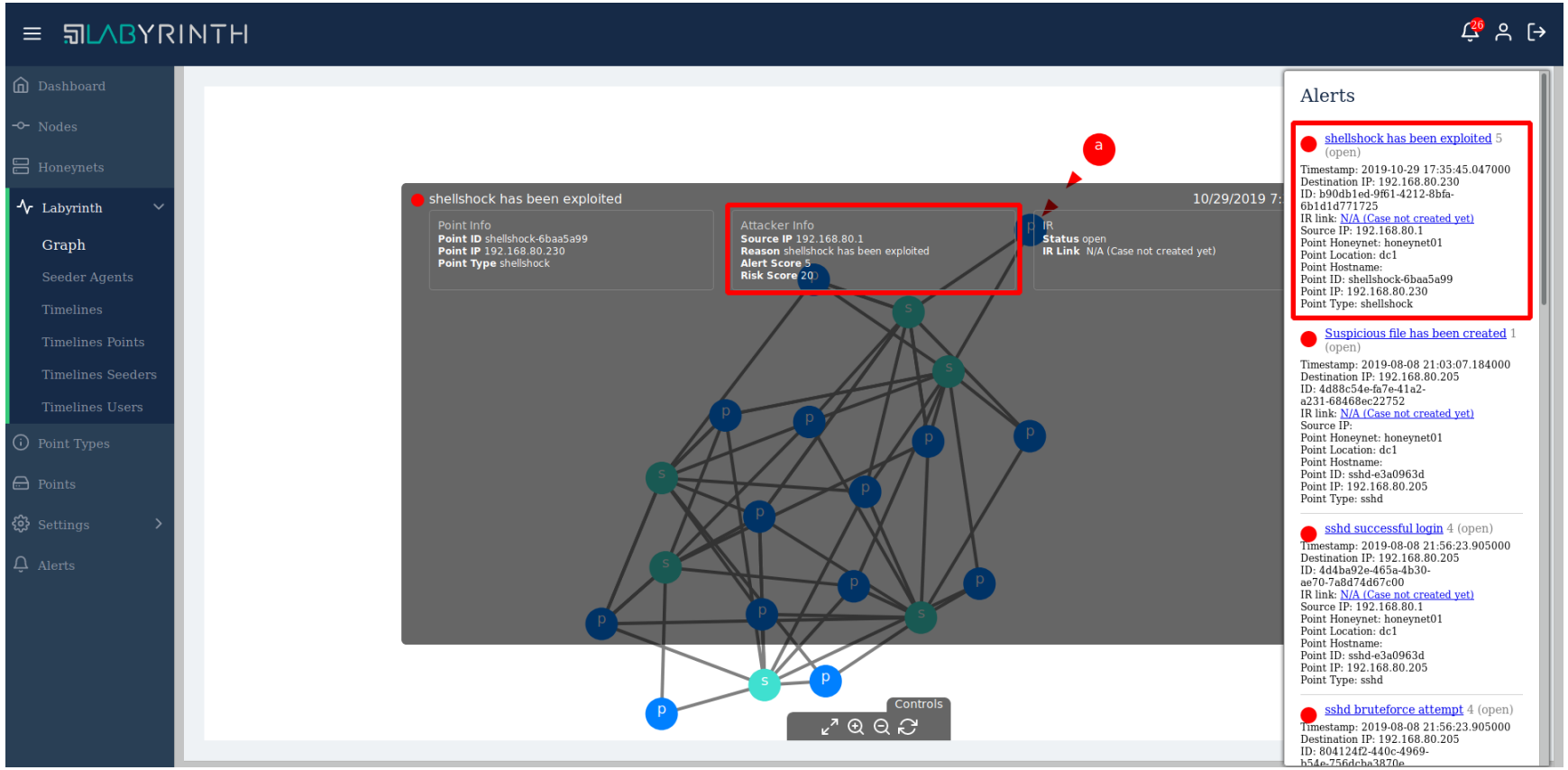
Виявлення

- **Рівень мережі**
- **Аномалії в протоколах**
- **Активність додатків**

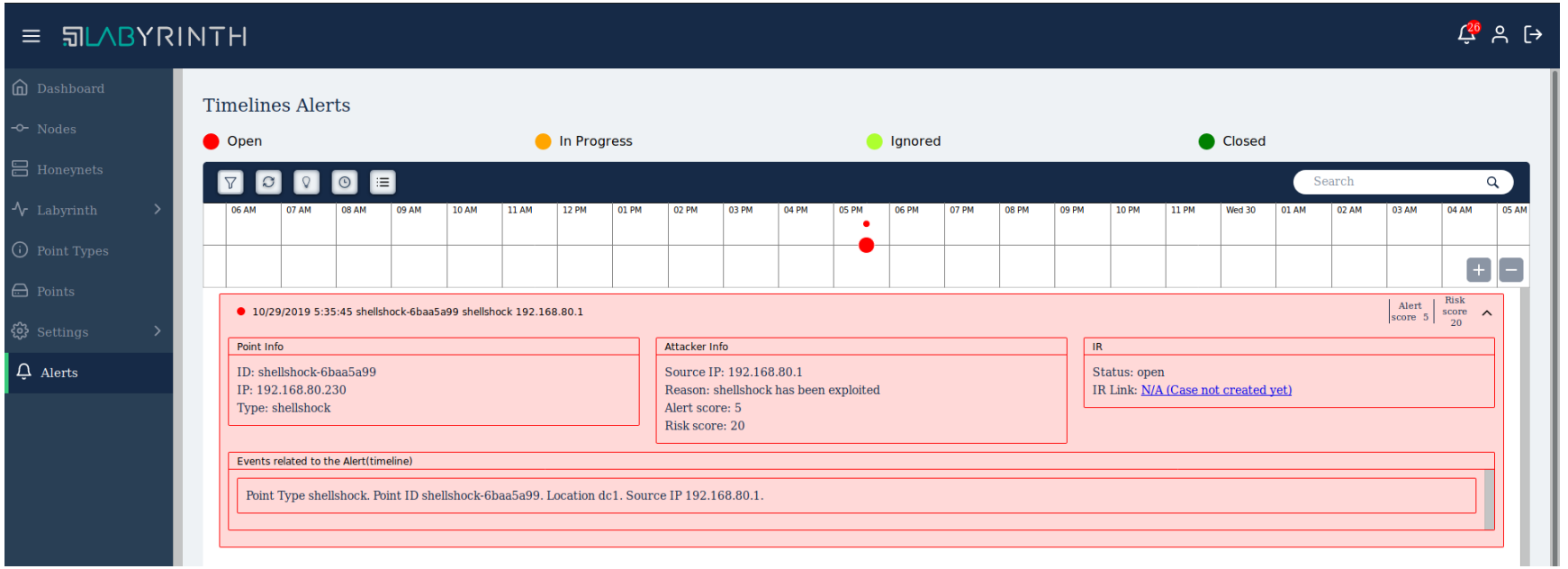


Сигналізація

- **Підозрілі активності**
- **Несанкціоновані спроби доступу**
- **Спроби використання вразливостей**



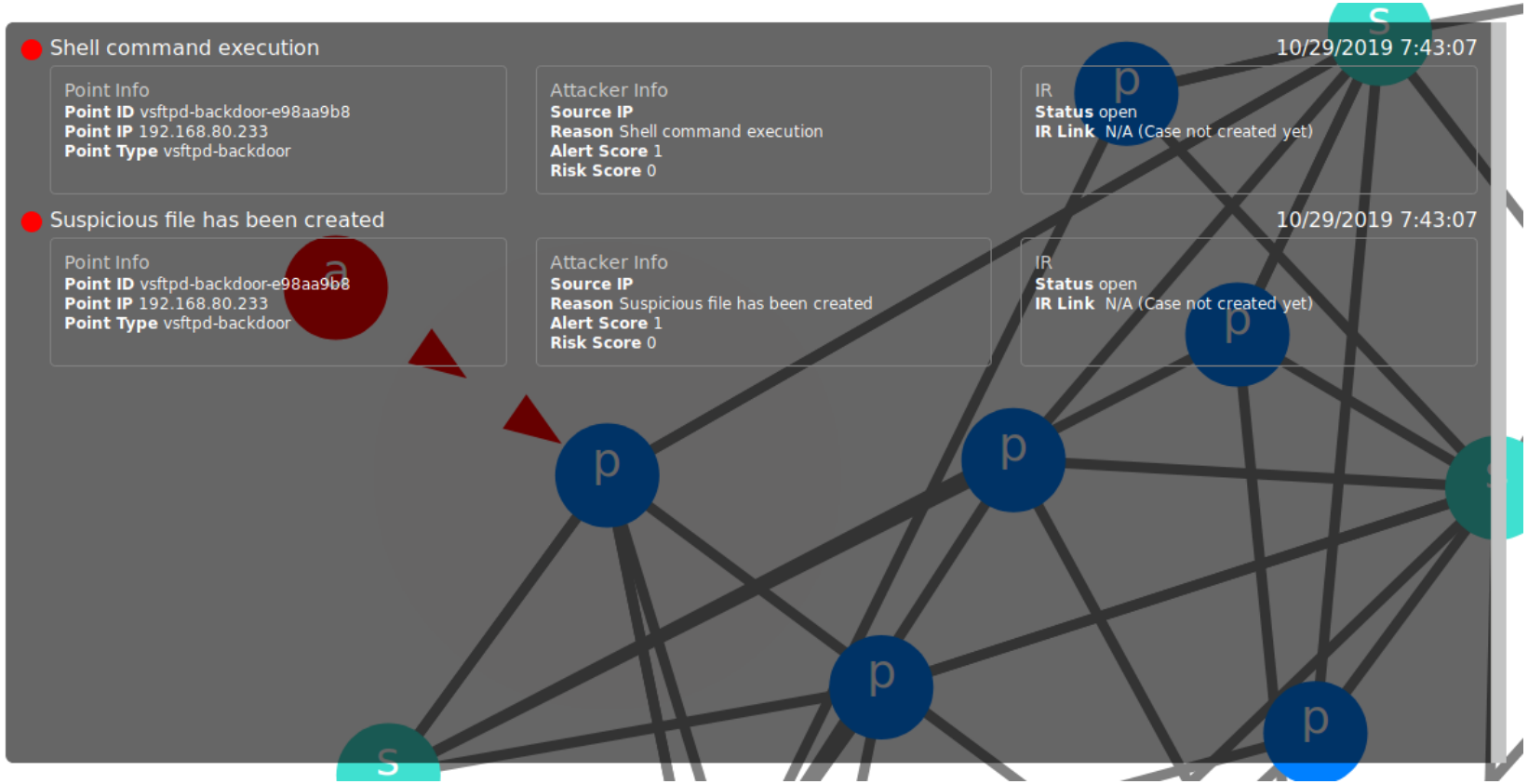
Збір даних



- **Збір даних з Points**
- **Ідентифікація загроз**
- **Логи інцидентів та звітність**
- **Інтеграція з SIEM**

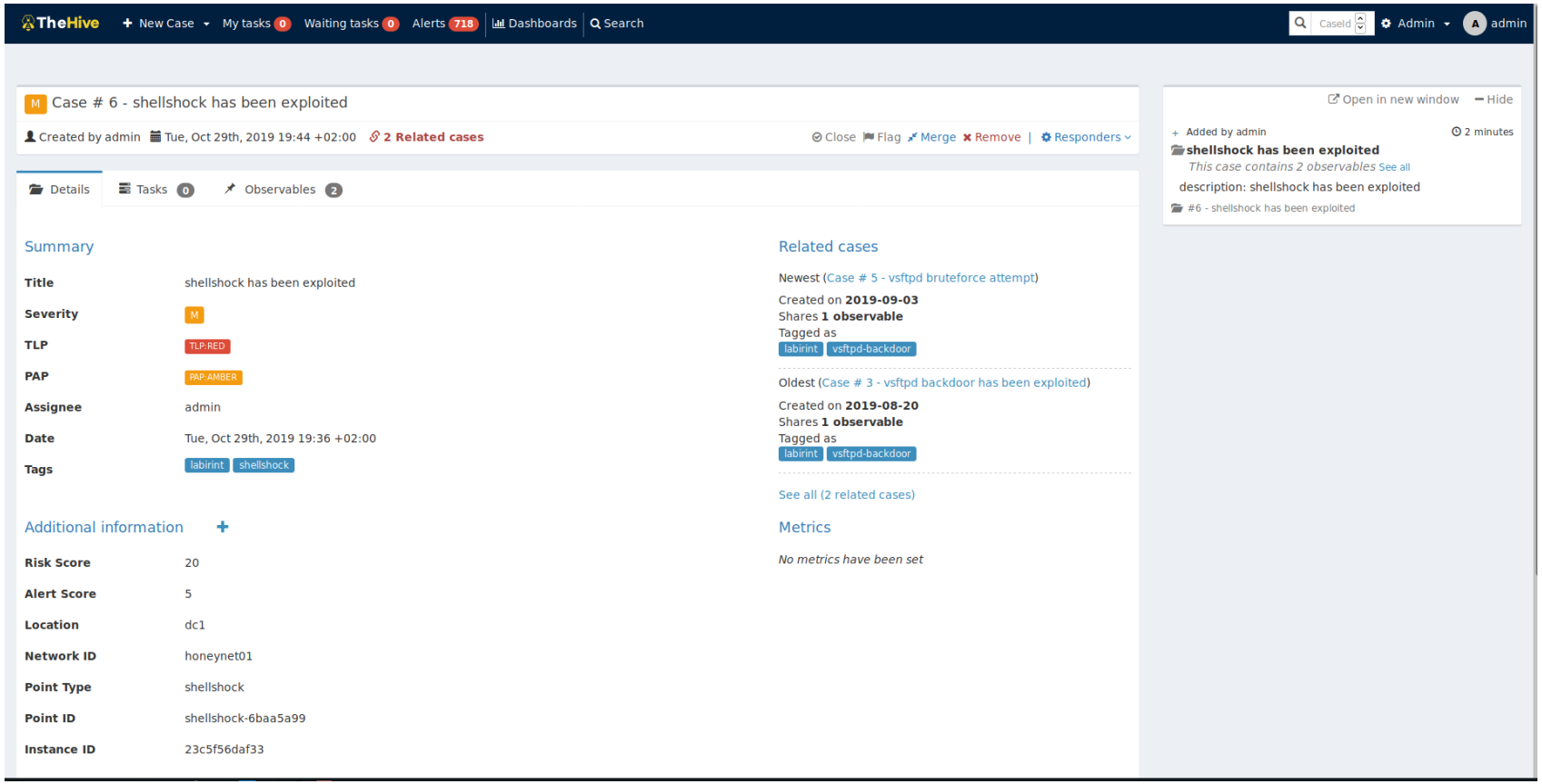
Аналіз

- **Аналіз шаблонів**
- **Спроби доступу**
- **Експлуатація вразливостей**
- **Аналіз поведінки**
- **Контент-аналіз**



Реагування

- **Підтримка розслідувань**
- **Автоматичне генерування індикаторів загрози**
- **Багатокористувацький доступ**
- **Створення звітності**
- **Автоматичне сповіщення**

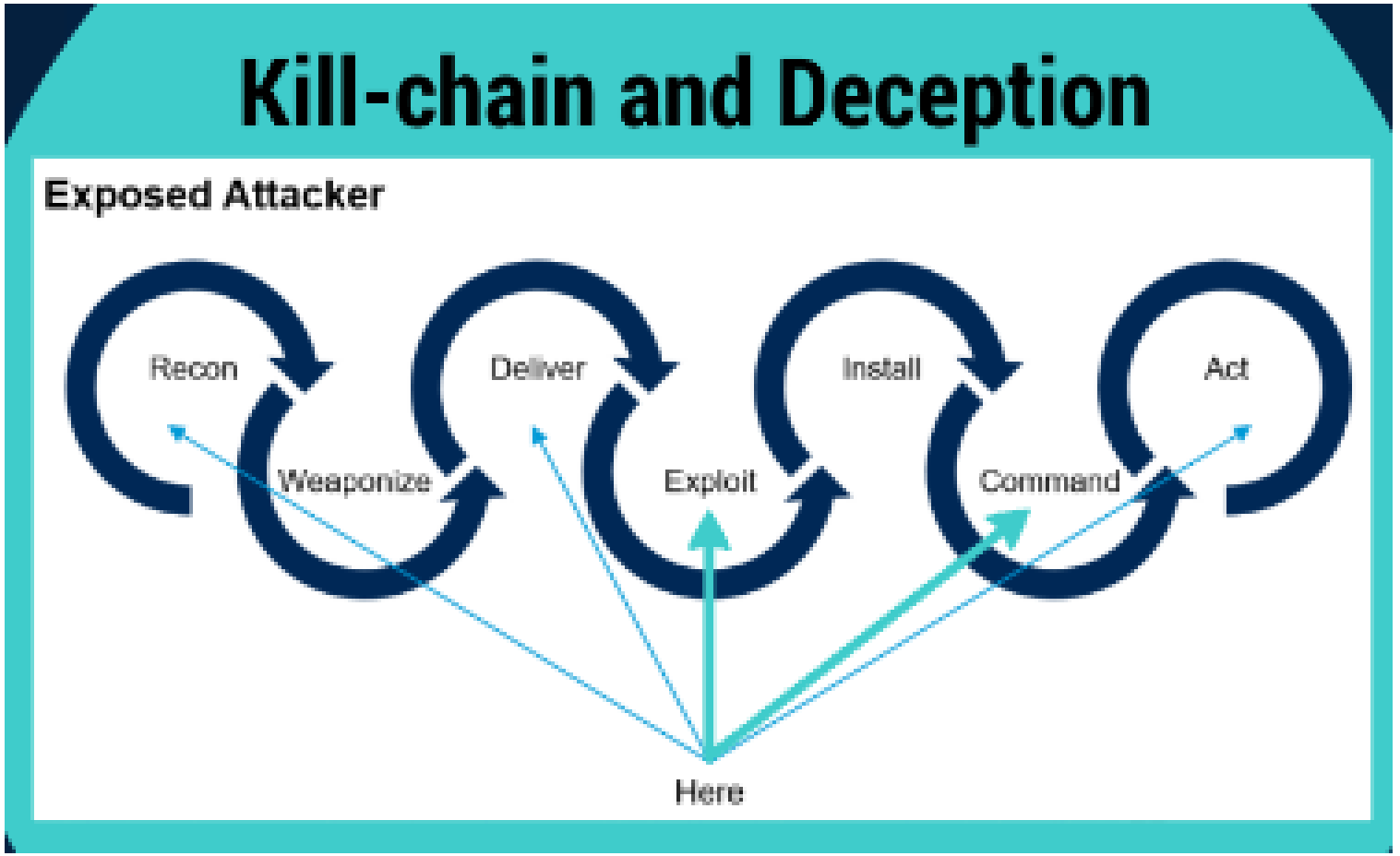


Переваги

- Раннє виявлення загрози в мережі
- Виявлення цільових атак
- Точні сповіщення
- Післяінфекційне виявлення
- Швидке реагування на інциденти
- Розпізнавання Lateral Movement
- Проактивний захист
- Скорочення Dwell Time

Особливості

- **Пастки високої взаємодії**
- **Різноманітність та автентичність Points**
- **Багатошарова безпека**
- **Кастомізація**
- **Автоматизація**
- **Маштабованість**



Зміна правил

На противагу більш традиційним підходам до безпеки, платформа Labyrinth Deception допомагає змінити правила гри на користь захисників.

Тепер нападники мають бути праві в 100% випадків, а захисникам, щоб їх зупинити, достатньо щоб пощастило всього один раз,.

Додаючи дуже ефективний рівень до поточних механізмів виявлення загроз, Labyrinth може виявити атаку, навіть якщо зловмисники ведуть себе дуже обережно не викликаючи реакцію в інших системах безпеки.

LABYRINTH

LABYRINTH DECEPTION PLATFORM

Створено для перемоги над хакерами

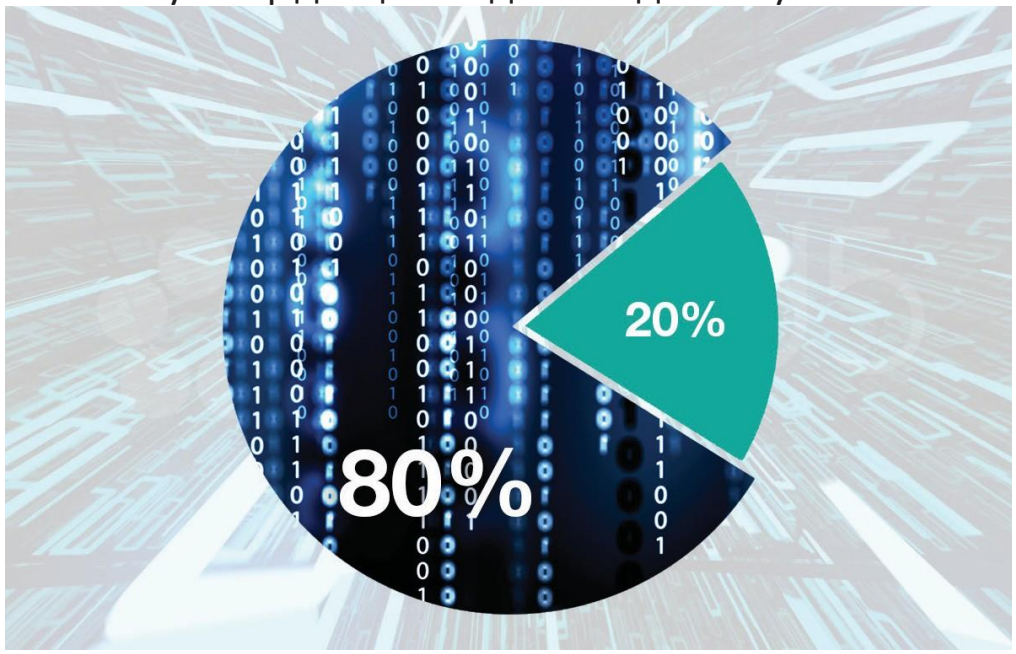
LABYRINTH

FIREWALLS ARE NOT ENOUGH

Хакінг з використанням скомпрометованих облікових даних користувачів, C2 та backdoor становить 80% усіх зломів.

Кіберзлочинці продовжують застосовувати більш просунуті та складні техніки злому.

Традиційних заходів безпеки, таких як брандмауер та захист кінцевих точок, недостатньо для зупинки хакерів та захисту конфіденційних даних від витоку.



51% усіх виявлених спроб вторгнення в інформаційні системи - це атаки без використання зловмисного програмного забезпечення.

56% вторгнень не виявляються протягом принаймні місяця.

60% підприємств за останні два роки зазнали серйозних інцидентів з кібербезпеки.

LABYRINTH

TRADITIONAL NETWORK THREAT DETECTION

Традиційні методи та техніки виявлення складних кіберзагроз здебільшого будуються на “big data” підході

Такі рішення вимагають інфраструктури, якою потрібно керувати, створюють величезну кількість оповіщень, які потребують розгляду, та інцидентів, які потребують розслідування кваліфікованим персоналом.

ПРОБЛЕМА КІЛЬКОСТІ

- високі витрати на централізацію логів та метадати
- дані займають багато місця при зберіганні
- аналітика даних вимагає багато обчислювальних ресурсів

ПРОБЛЕМА ОБРОБКИ

- надмірна кількість сповіщень, які потребують обробки
- високий показник помилково-позитивних сповіщень
- неможливість розставити пріоритети для інцидентів

ПРОБЛЕМА ЕКСПЕРТИЗИ

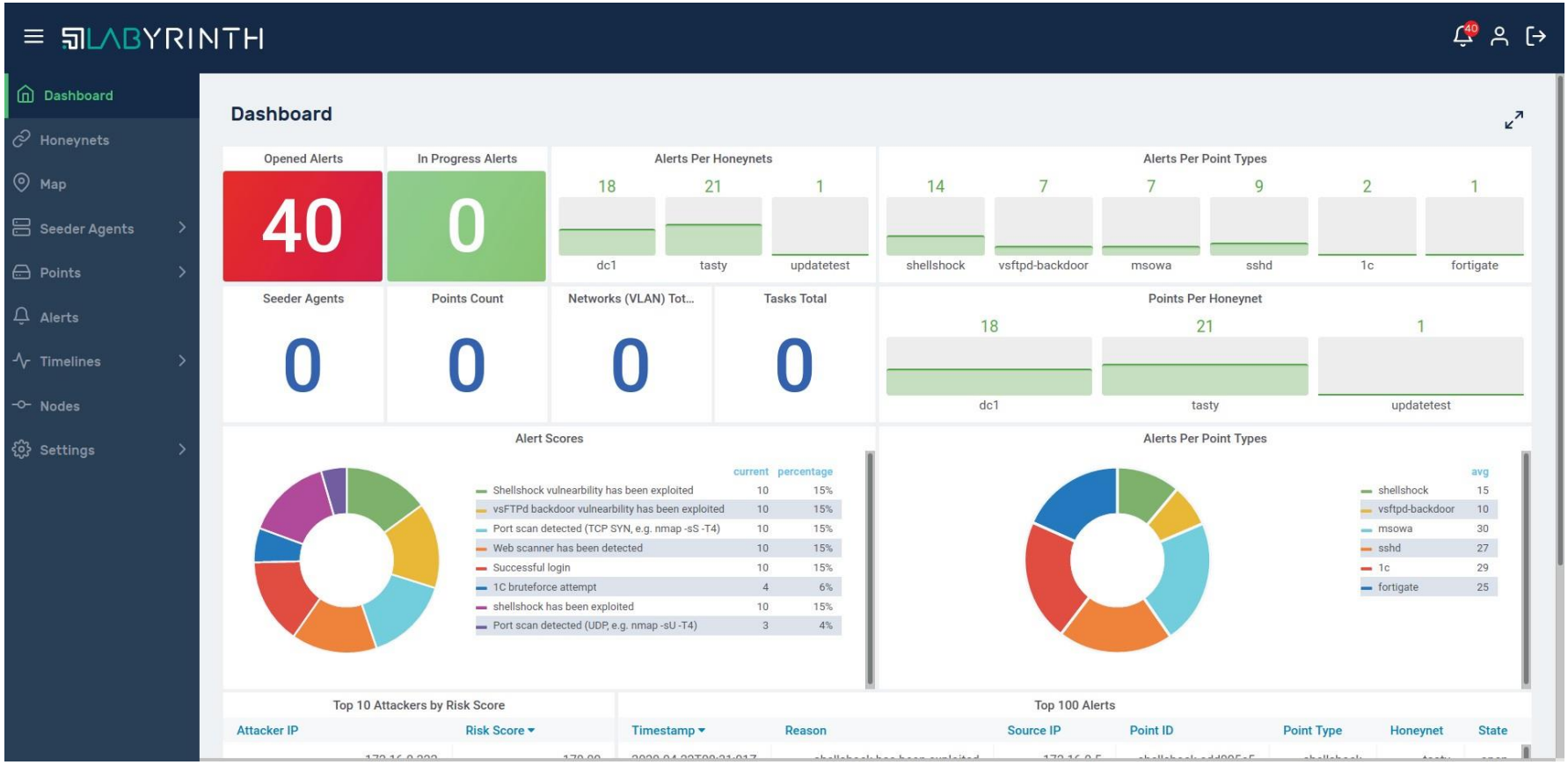
- відсутність кваліфікованого персоналу
- висока вартість навченого персоналу
- неадекватна реакція на інциденти

Security Teams витрачають більше 25% свого часу розбираючи False Positive оповіщення (Ponemon Institute research 2020)

LABYRINTH

DECEPTION-BASED THREAT DETECTION

Labyrinth Deception Platform змінює парадигму кібербезпеки, підходячи до виявлення загроз як до проблеми "правильних даних", а не "великих даних"



Платформа збирає тільки дані з власних сенсорів та генерує лише високоточні сповіщення, які побудовані в інциденти та збагачені контекстом.

LABYRINTH

LABYRINTH DECEPTION PLATFORM ADVANTAGES

Детектування складних загроз

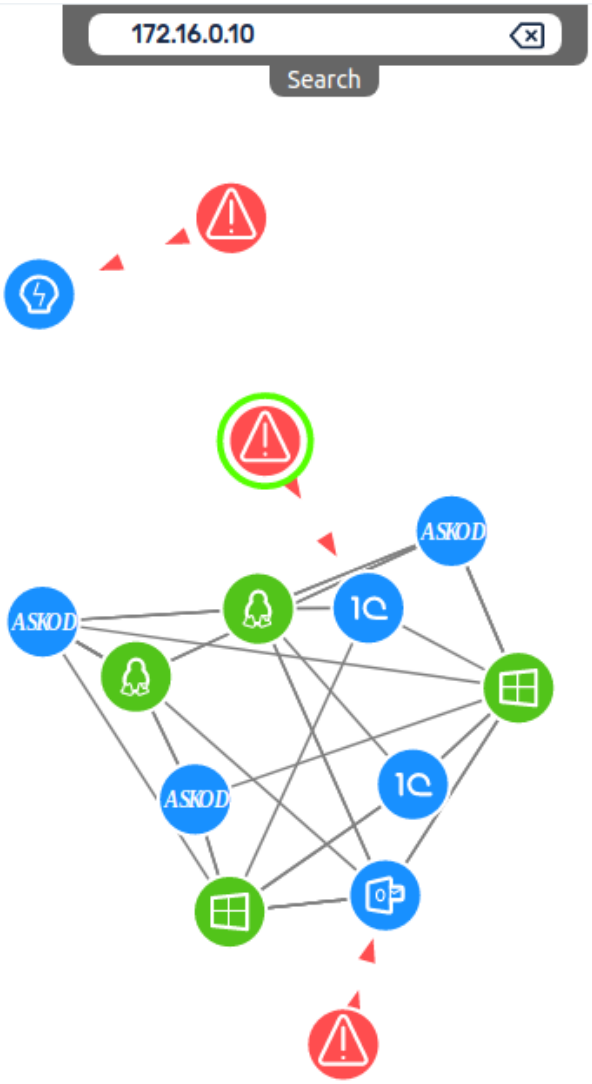
- Дозволяє виявити зловмисників у корпоративній мережі до 12 разів швидше
- Виявляє базові та складні загрози, незалежно від використовуваних технік
- Збирає дані про переміщення атакуючих та застосовані ними інструменти

Оптимізація процесів SOC

- Значно спрощує процес пріоритезації інцидентів
- Скорочує час витрачений на помилково позитивні сповіщення
- Забезпечує повну видимість атаки в режимі реального часу

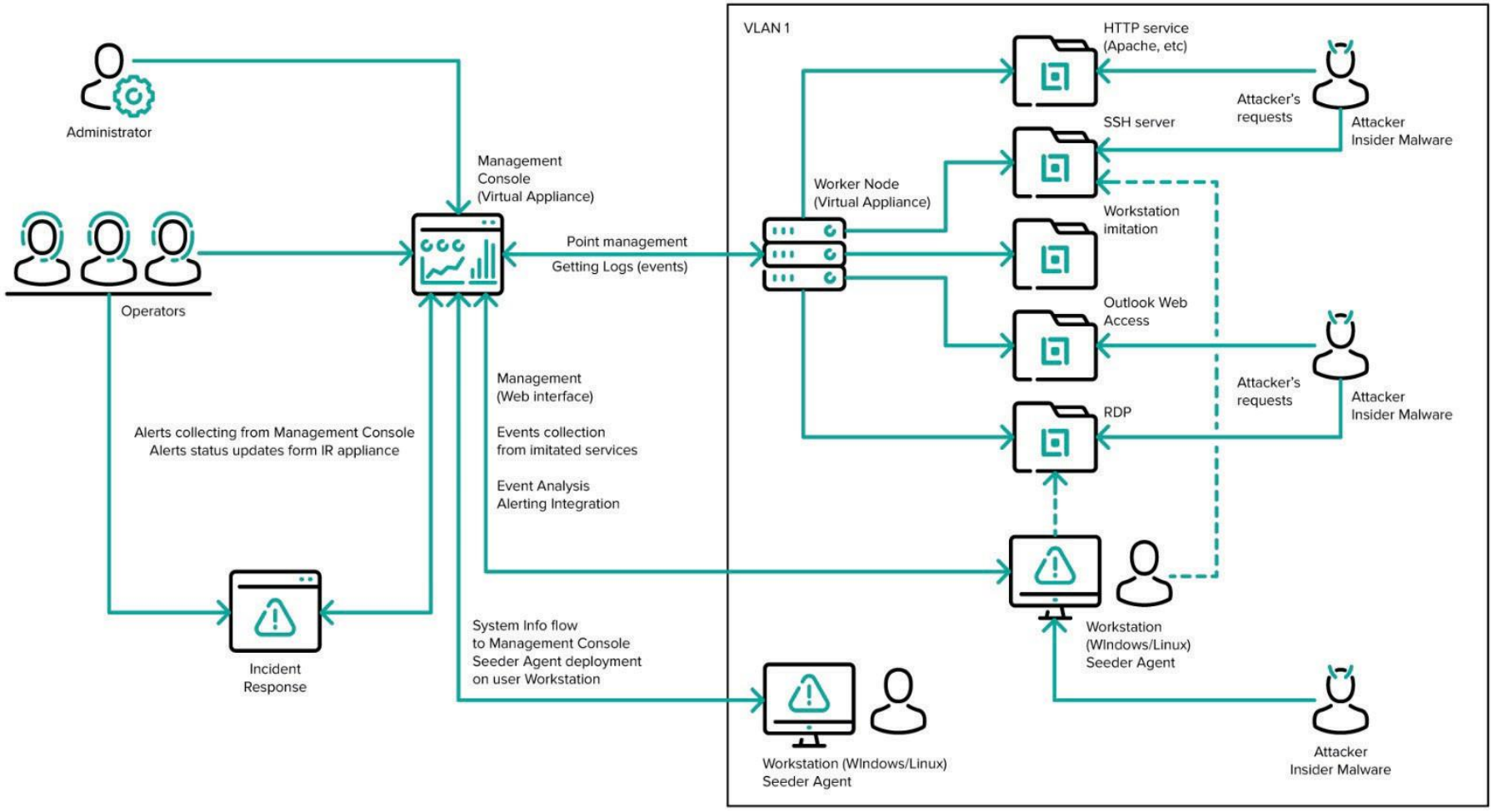
Зниження складності

- Проста установка та конфігурація
- Ніяких спеціальних навичок для користування рішенням
- Автоматизоване виявлення та реагування



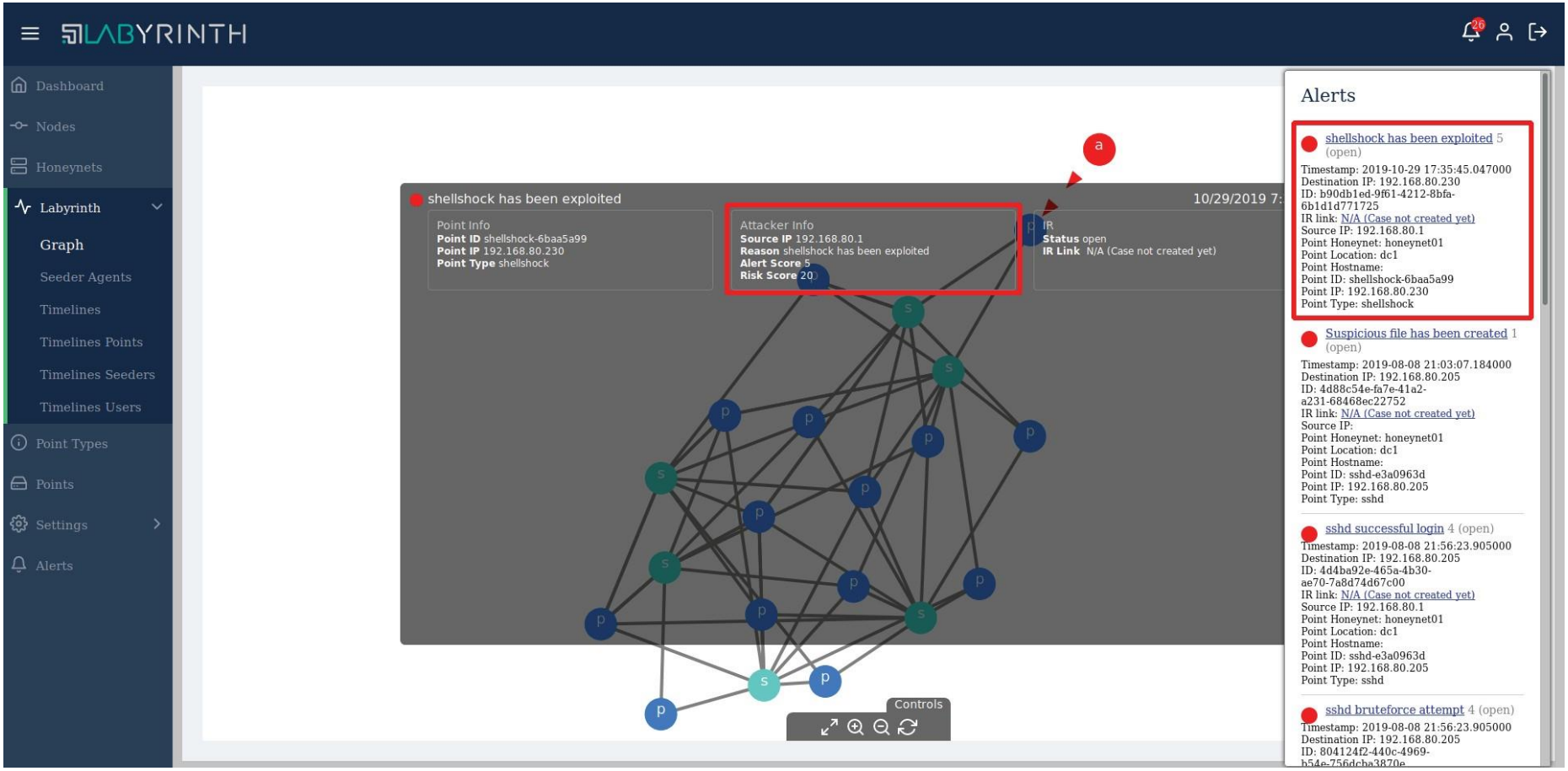
LABYRINTH DECEPTION PLATFORM

Платформа створює вразливі IT сервіси та додатки, в рази збільшуючи площу атаки та дезорієнтуючи атакуючих. Labyrinth провокує зловмисників на дії, виявляє та відстежує всю їхню діяльність та ізолює їх від реальної IT-мережі.



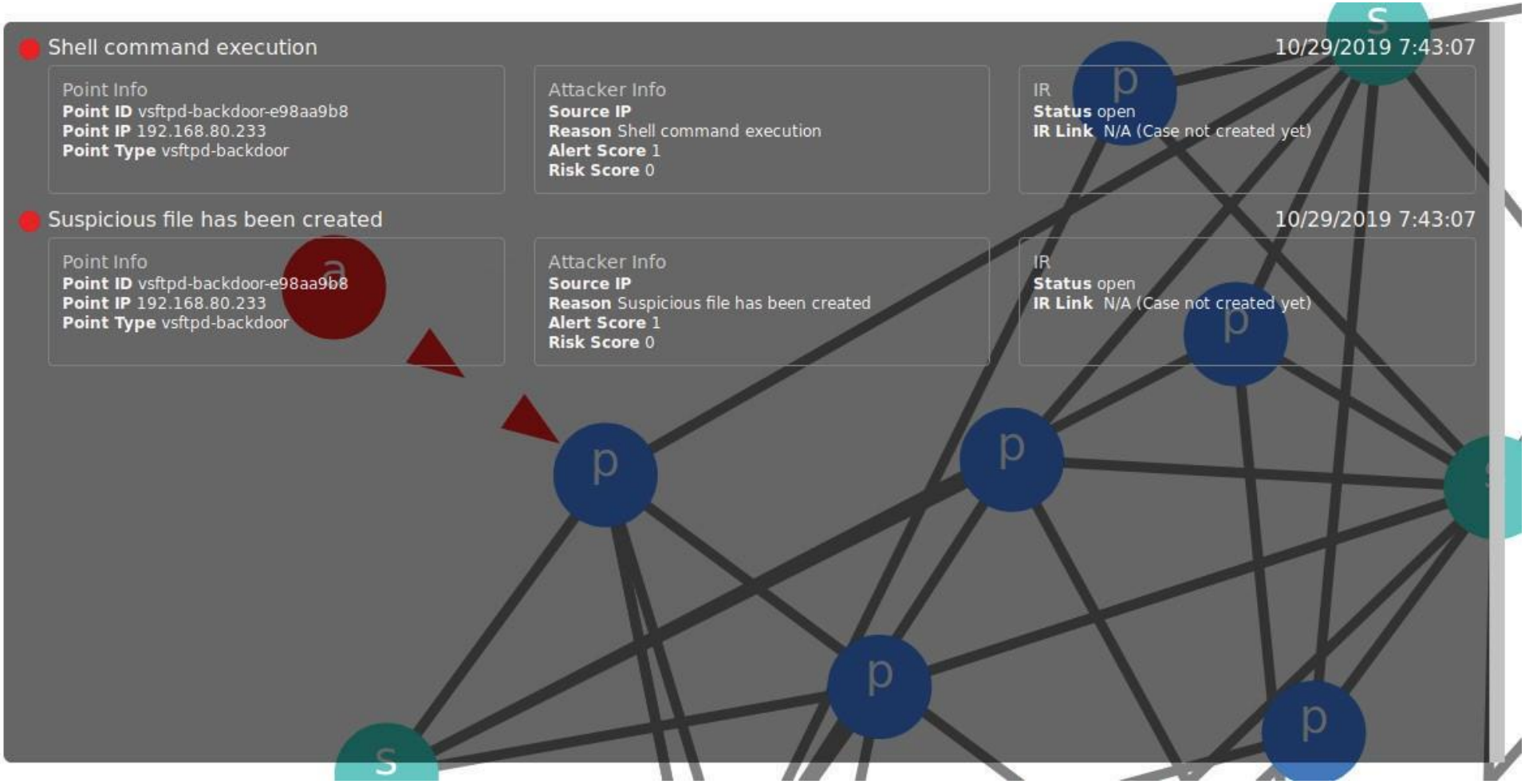
KEY CAPABILITIES: THREAT DETECTION

- Розвідувальна діяльність
- Спроби несанкціонованого доступу
- Експлуатація вразливостей
- Command and Control атаки



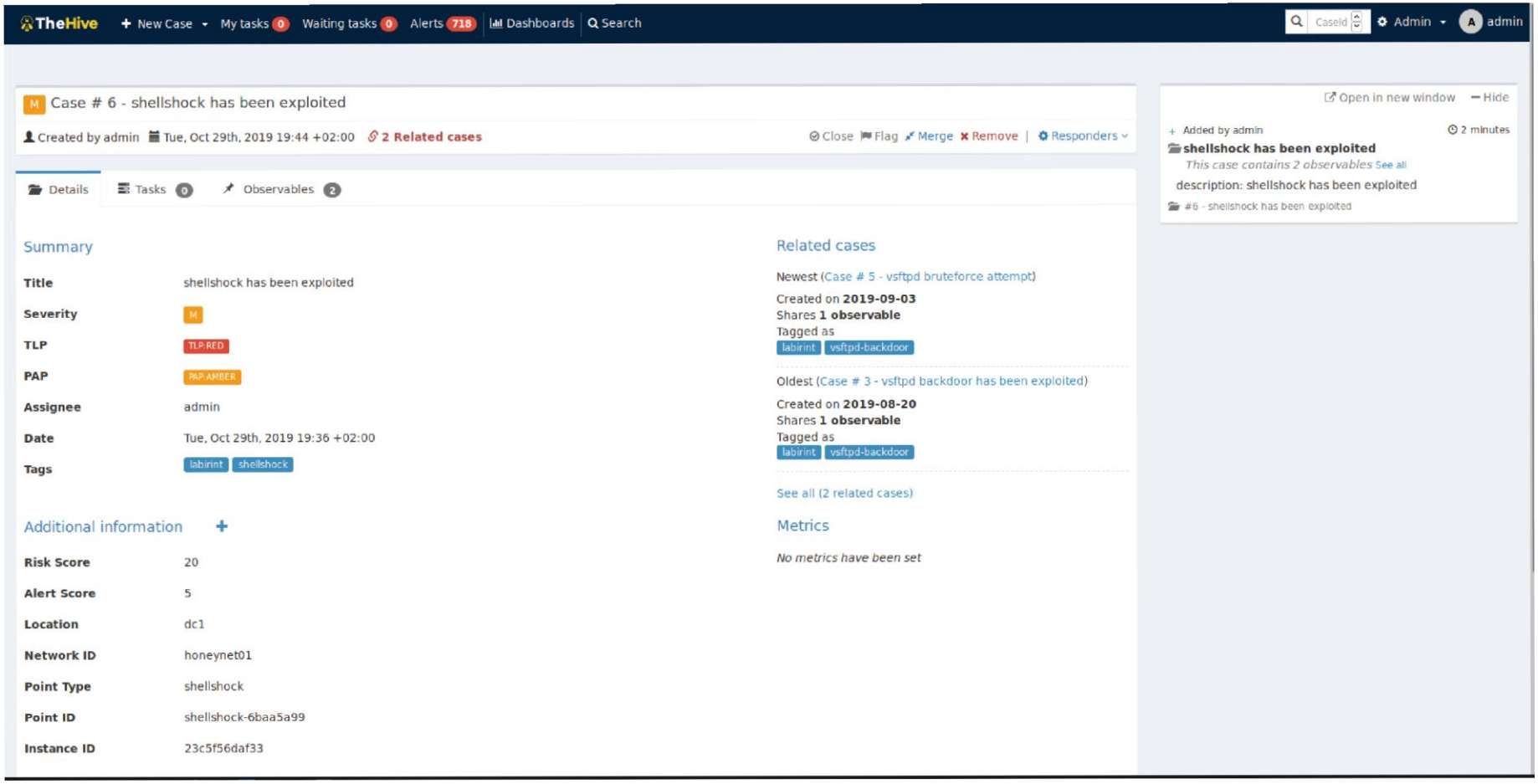
KEY CAPABILITIES: THREAT ANALYSIS

- Агрегація сповіщень
- Аналіз поведінки
- Спроби доступу
- Аналіз контенту



LABYRINTH KEY CAPABILITIES: AUTOMATED RESPONSE

- Повна підтримка розслідувань
- Ізоляція скомпроментованих хостів
- Автоматична генерація індикаторів загроз
- Створення звітів



LABYRINTH

INTEGRATIONS

LABYRINTH

UNIQUE FEATURES

Розширені можливості виявлення

Платформа надає зловмисникам широкий спектр фальшивих вразливостей програм та служб, щоб збільшити поверхню атаки та забезпечити охоплення всіх можливих векторів атак.

Розширений захист WEB-додатків

Лабіринті використовує унікальну технологію, яка дозволяє забезпечити додатковий рівень захисту для найбільш бажаної цілі хакерів - WEB-додатки та сервісів.

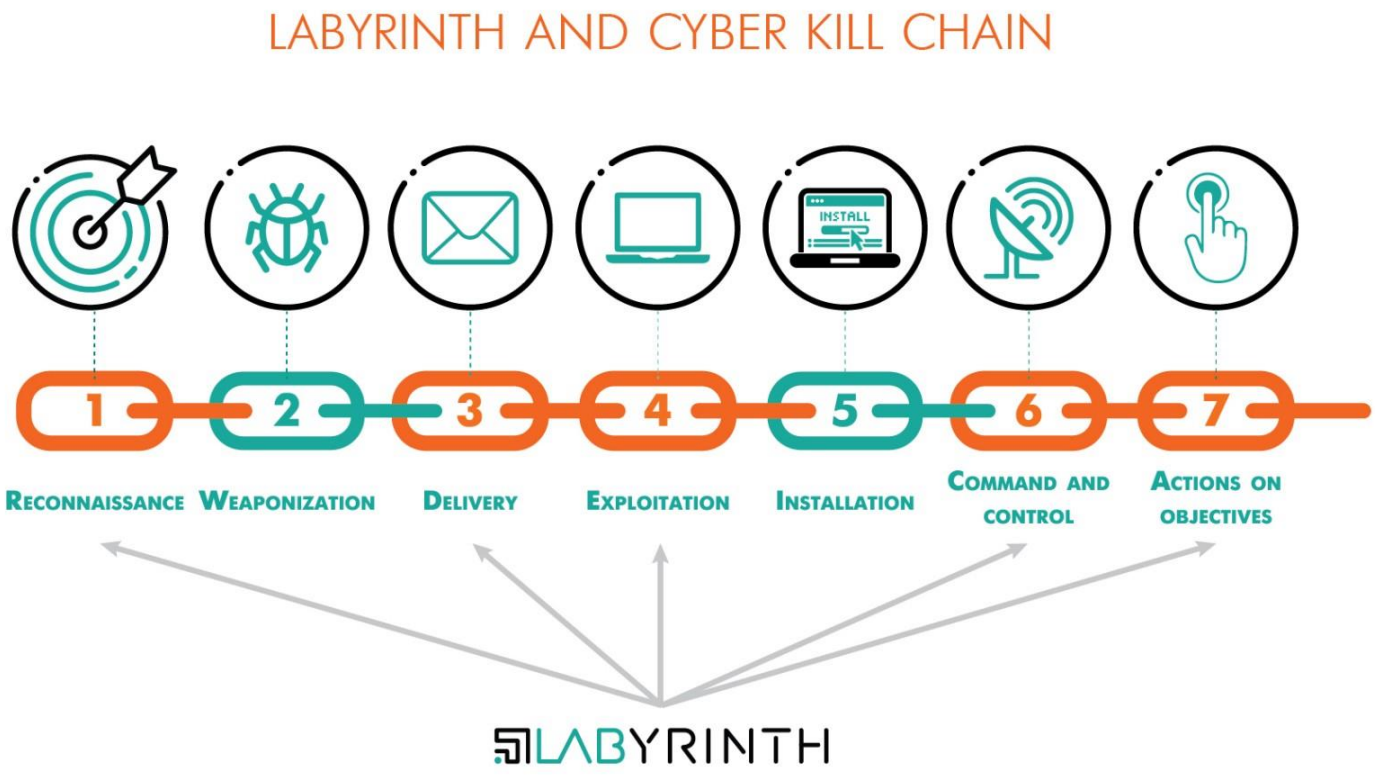
Активний захист

Клієнтські Honeypots - це активні пристрої безпеки, які використовуються для пошуку шкідливих серверів, що атакують клієнтів та виявлення MITM. Вони поводяться як клієнт і перевіряють, чи сталася атака.

LABYRINTH

USE CASES

- Раннє виявлення загроз в мережі
- Проактивний захист
- Виявлення цільових атак
- Скорочення Dwell Time
- Детектування Man-In-the-Middle
- Розпізнавання Lateral Movement
- Швидке реагування на інциденти
- Розслідування інцидентів



LABYRINTH

BUSINESS VALUE

ЗУПИНЯЄ СКЛАДНІ ЗАГРОЗИ

Виявляє цільові та розширені атаки, не вимагаючи попередніх знань про форму, тип чи поведінку загрози.

НУЛЬОВИЙ ВПЛИВ НА ПРОДУКТИВНІСТЬ

Немає негативного впливу на продуктивність мережевих пристроїв, хостів, серверів чи програм.

ПРОСТЕ ВПРОВАДЖЕННЯ

Швидке та просте розгортання без системних конфліктів та з мінімальним обслуговуванням - без баз даних, сигнатур чи правил для налаштування та оновлення

ЗНИЖЕННЯ ОПЕРАЦІЙНИХ ВИТРАТ ДО 30%

Не збирає тони даних, не генерує помилкові позитивні сповіщення, не потрібно спеціальних навичок для роботи.

АВТОМАТИЗАЦІЯ РЕАКЦІЇ НА ІНЦИДЕНТИ

Прискорює реагування на інциденти, скорочуючи середній час виявлення та реагування (MTTD, MTTR) в **12 РАЗІВ**

LABYRINTH

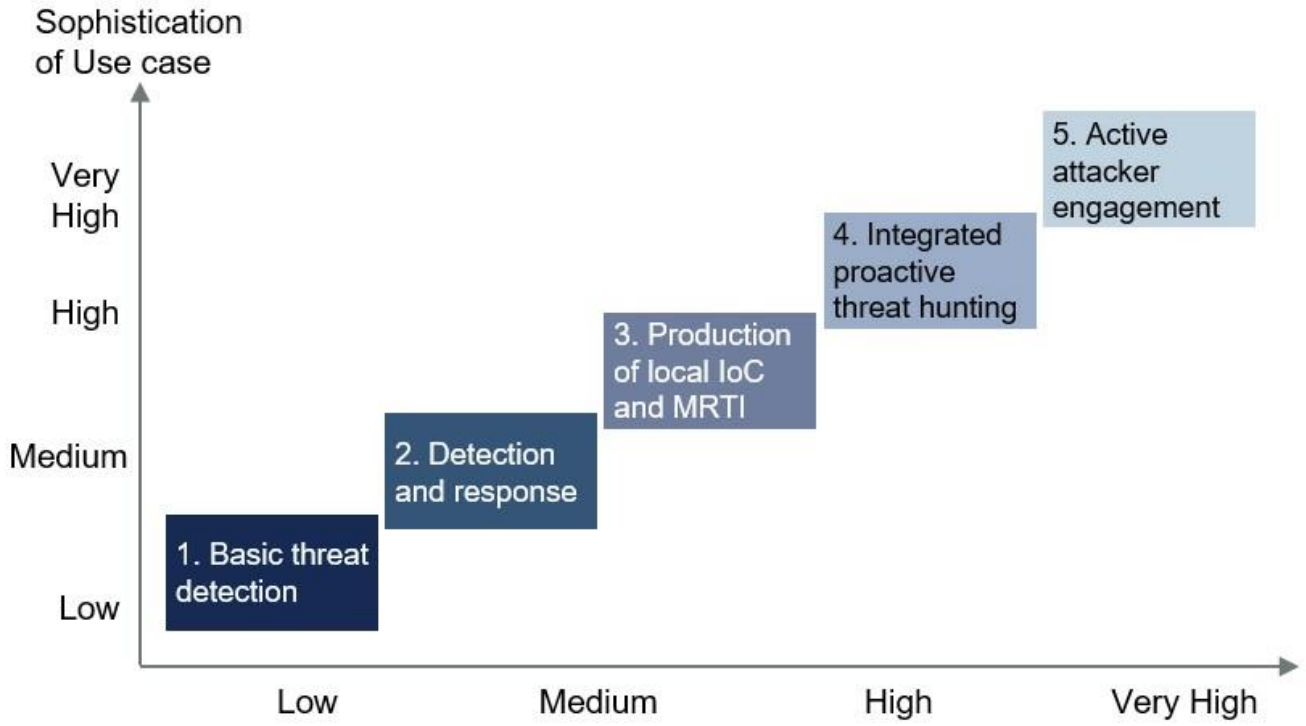
CHANGE THE GAME

На противагу більш традиційним підходам до безпеки, платформа Labyrinth Deception допомагає змінити правила гри на користь захисників.

Тепер нападники мають бути праві в 100% випадків, а захисникам, щоб їх зупинити, достатньо щоб пощастило всього один раз.

Додаючи дуже ефективний рівень до поточних механізмів виявлення загроз, Labyrinth може виявити та зупинити атаки які обійшли захист периметру мережі.

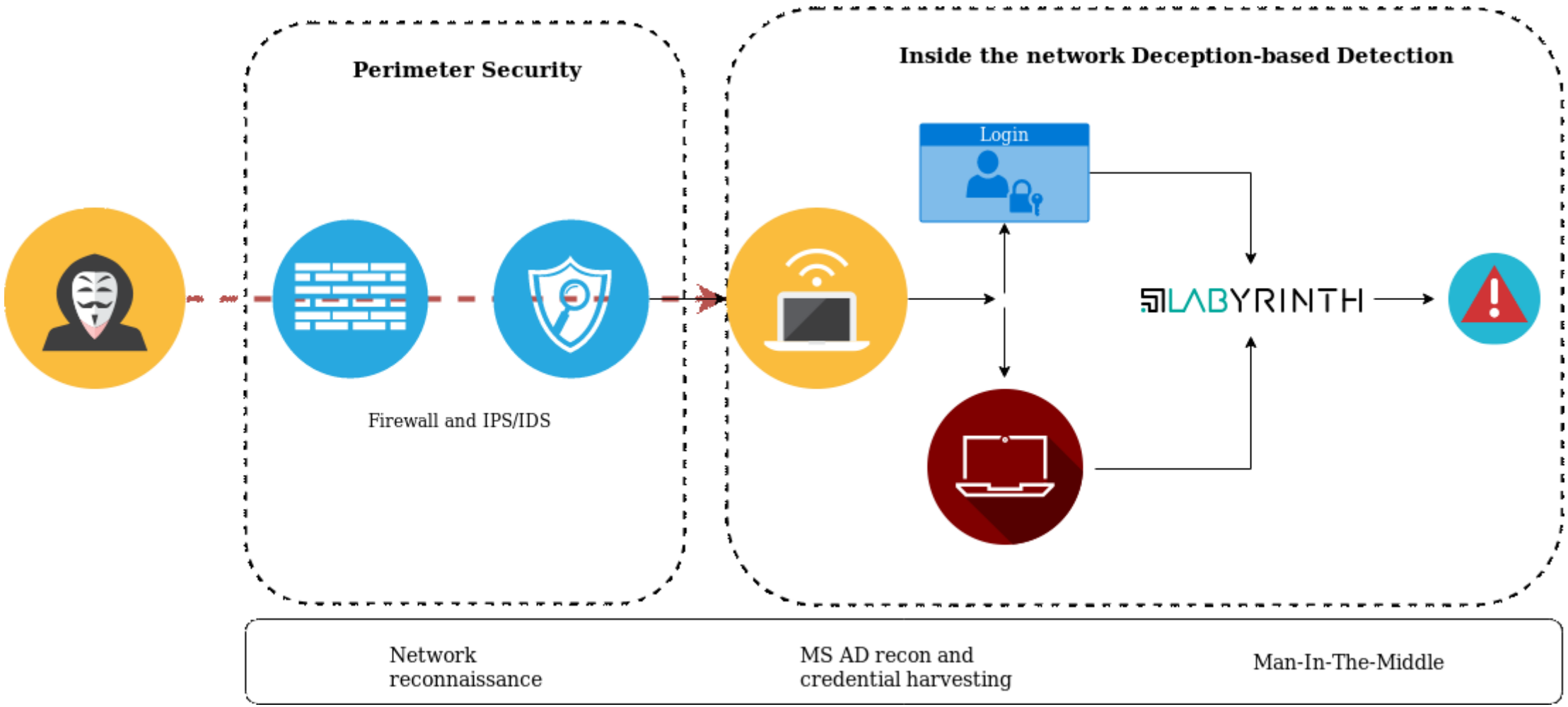
The Five Use Cases of Deception



“Спеціалісти з управління безпекою та ризиком, які шукають інструменти для розробки або розширення функцій виявлення та реагування на загрози, повинні включити в свій стек інструменти Deception."

Gartner, Improve Your Threat Detection Function With Deception Technologies, 2019

Labyrinth Deception Platform



Основні складові платформи

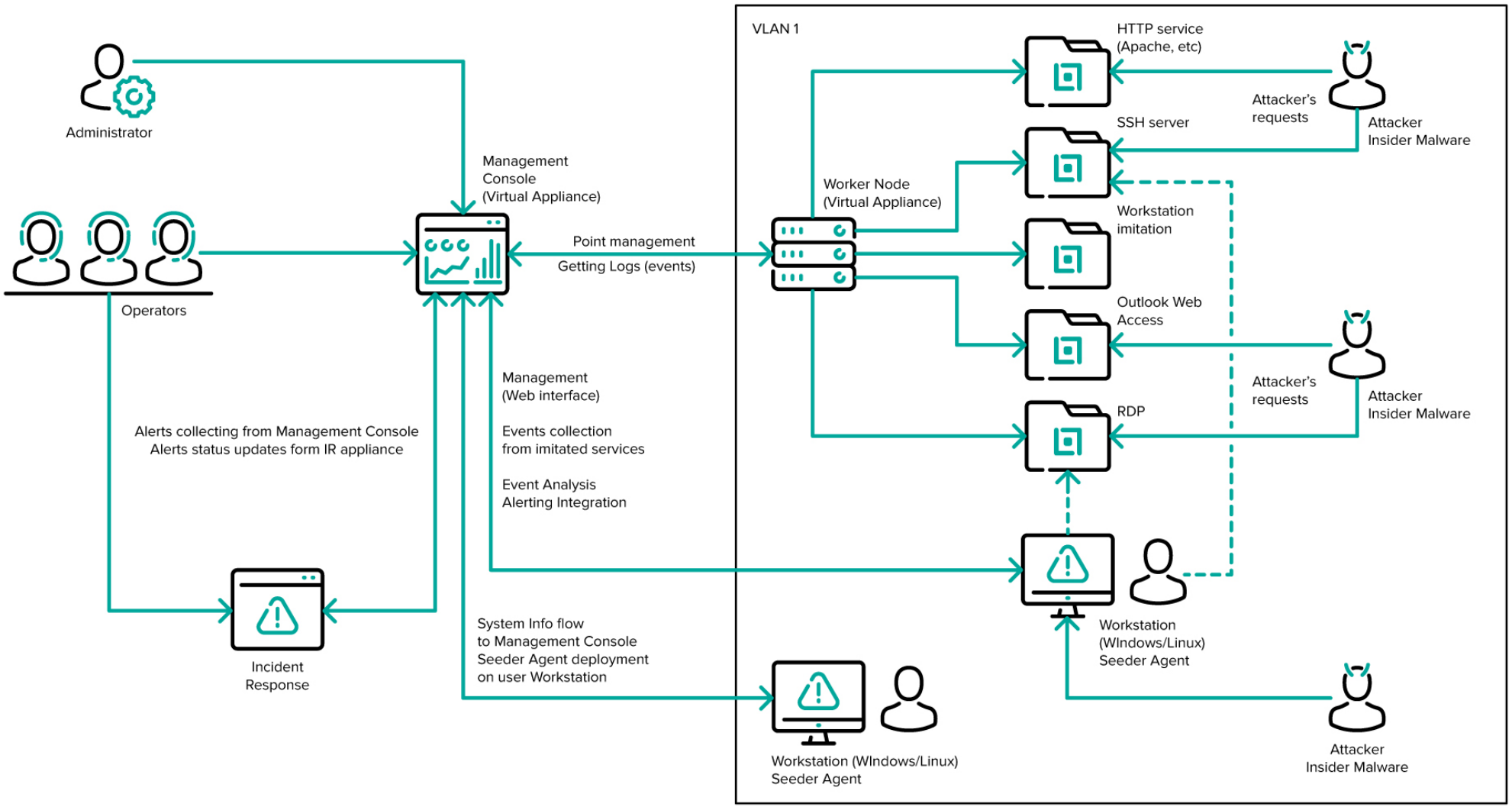
Point

Admin Console

Seeder агенти

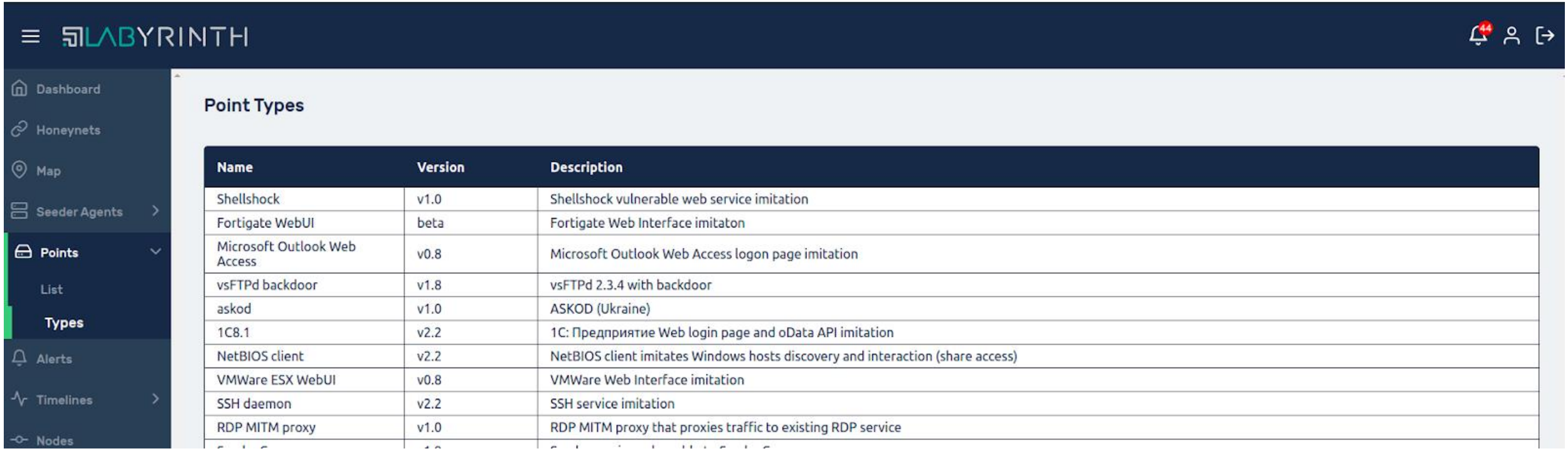
Worker

Архітектура рішення Labyrinth

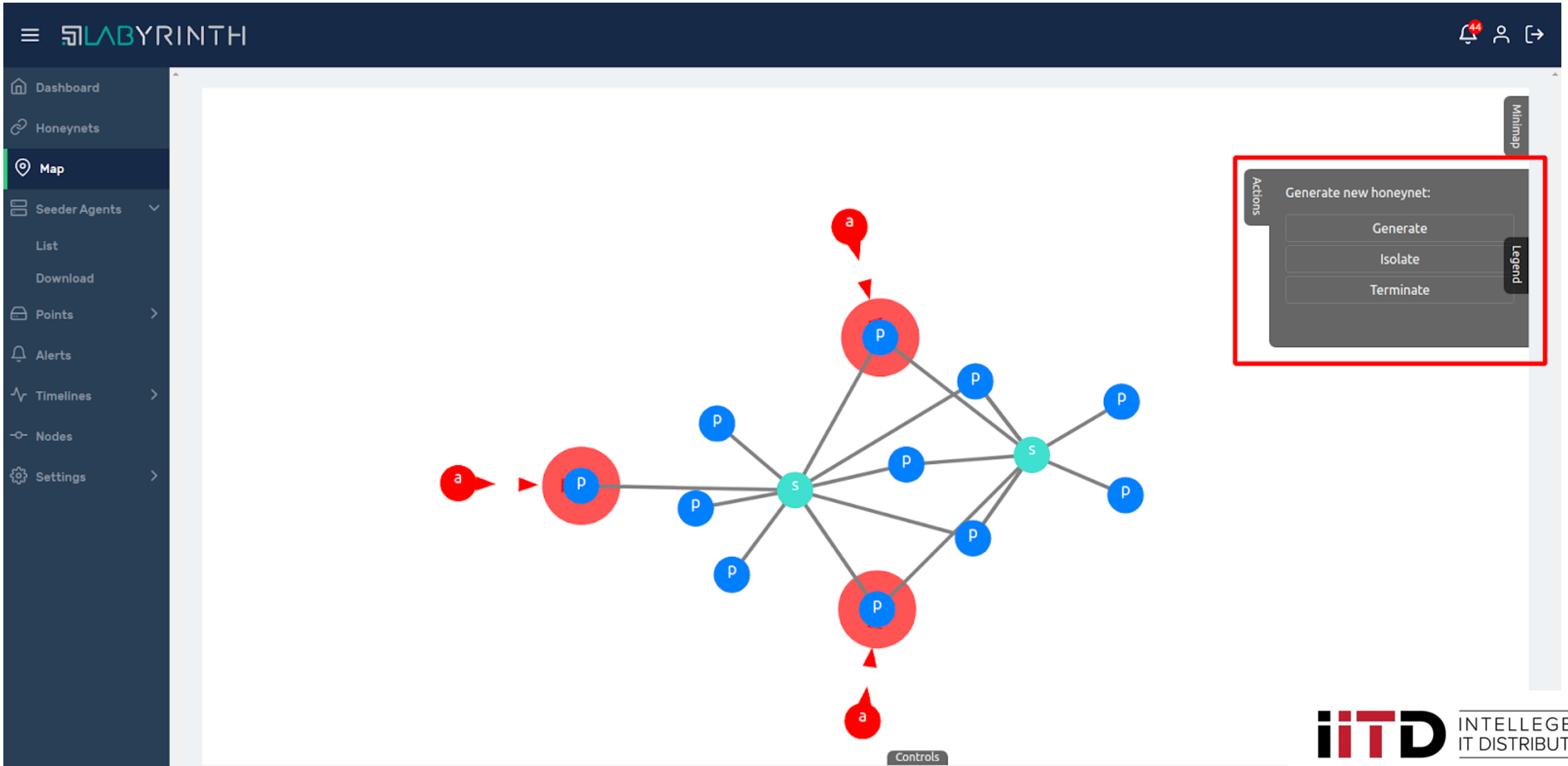


INTELLEGENT IT DISTRIBUTION

Розширення різноманітності типів Point

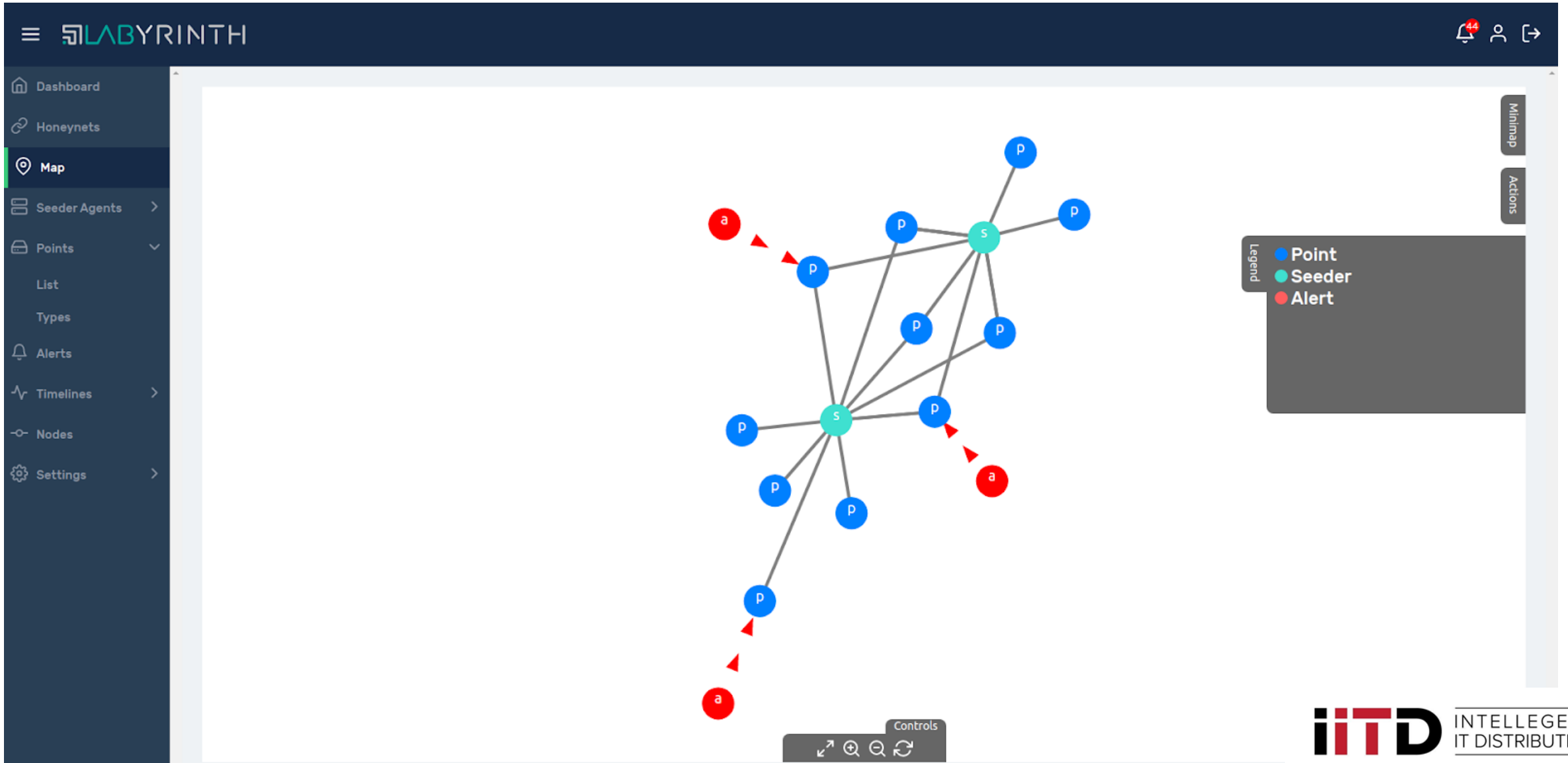


Керування системою

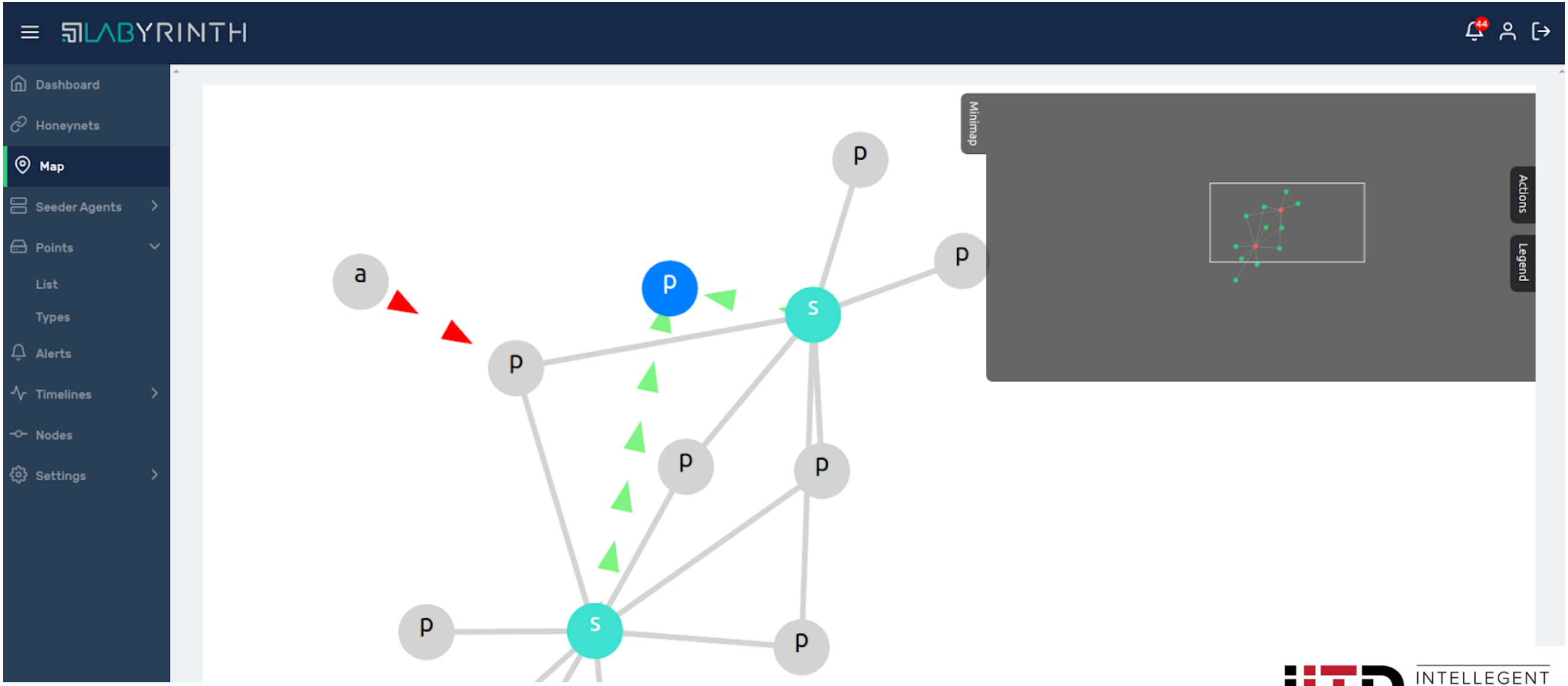


INTELLEGENT IT DISTRIBUTION

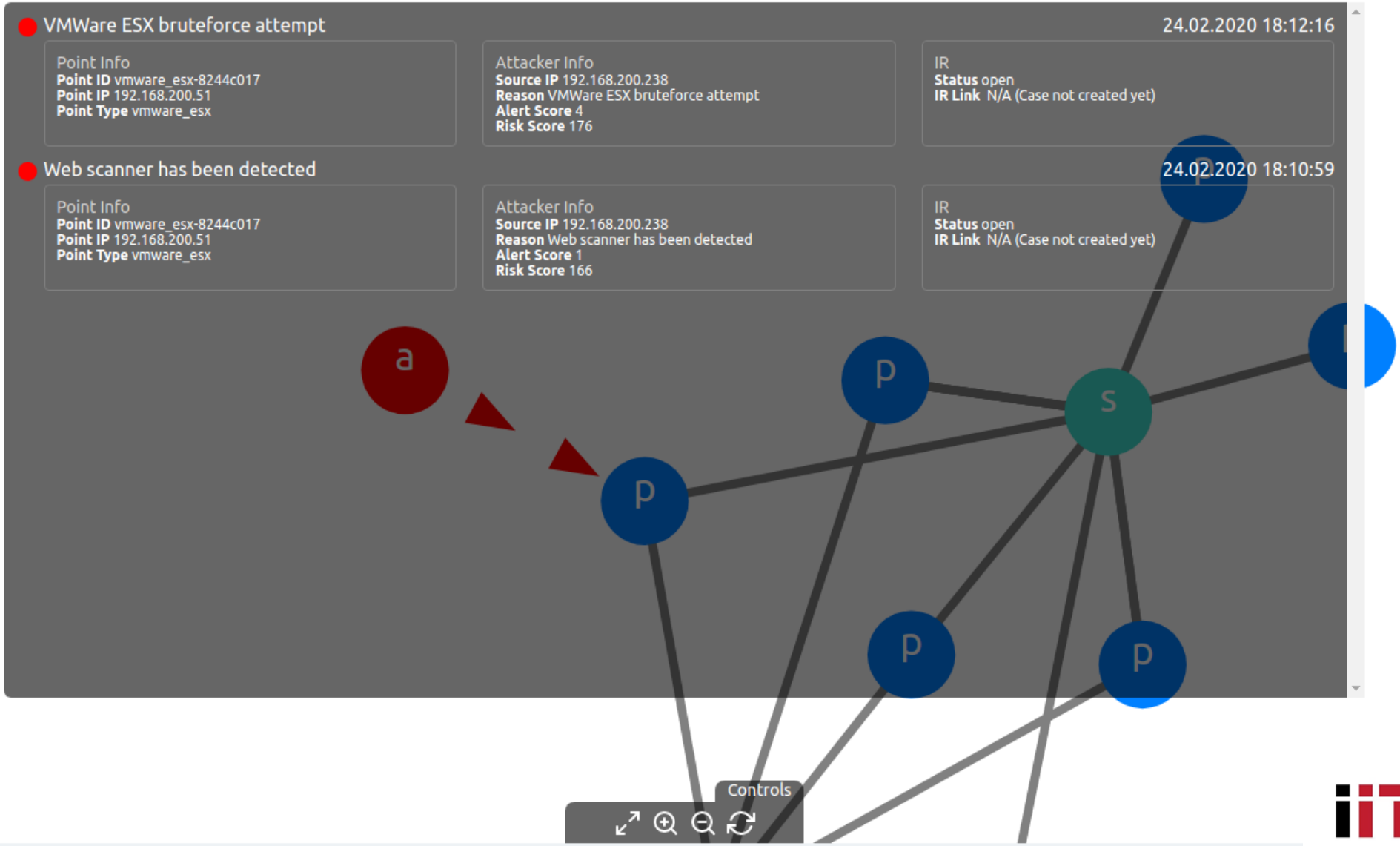
Візуалізація інцидентів



Взаємодія реальних та імітованих систем

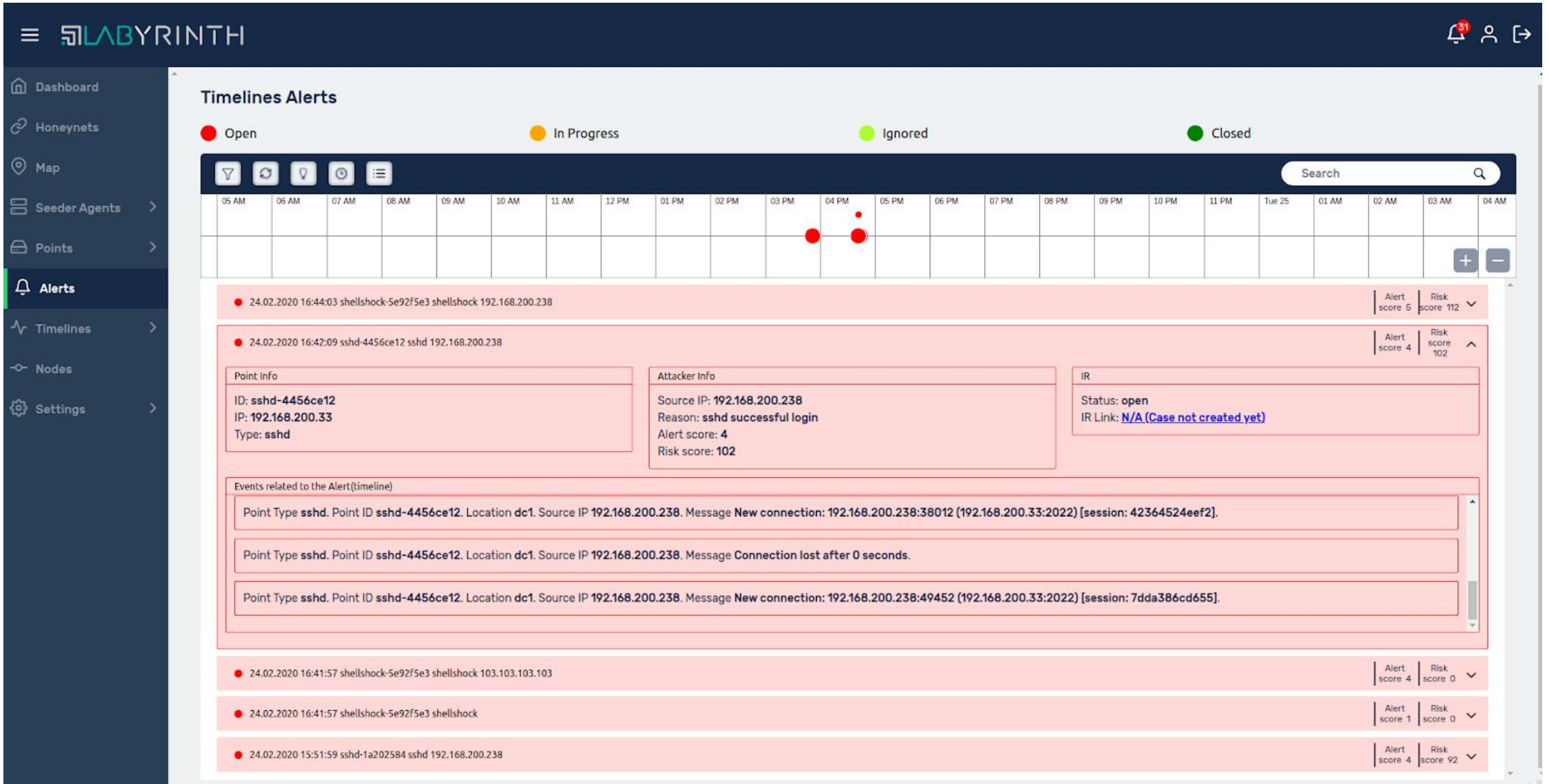


Агрегація даних про різнотипні атаки на Point



INTELLEGENT IT DISTRIBUTION

Відображення послідовності атак та їх зміст



Постійне оновлення і вдосконалення системи