R-Vision

# Threat Deception Platform

www.rvision.ru

# Предпосылки появления технологий кибероbмана

Инфраструктуры большинства организаций **уже скомпрометированы**

Киберпреступникам все проще проникнуть в инфраструктуру **и дольше оставаться незамеченными***

**Рост числа 0-day угроз и APT-атак** в мире, в том числе международных

Системы обнаружения **не учитывают специфику отраслей** и особенностей инфраструктур заказчиков

* Согласно отчету Cost of a Data Breach Report 2021, время обнаружения различных угроз в инфраструктуре - от 150 до 250 дней

# HONEYPOTS

Привлечение внимания - используются только ловушки

Статичная конфигурация

Анализ действий злоумышленника

Быстро распознаются опытными хакерами

Каждая ловушка внедряется и поддерживается вручную

# DECEPTION

Привлечение внимания, **запутывание и обман** злоумышленника благодаря взаимосвязанным приманкам и ловушкам

Динамическая адаптация под инфраструктуру

Обнаружение и замедление развития атаки

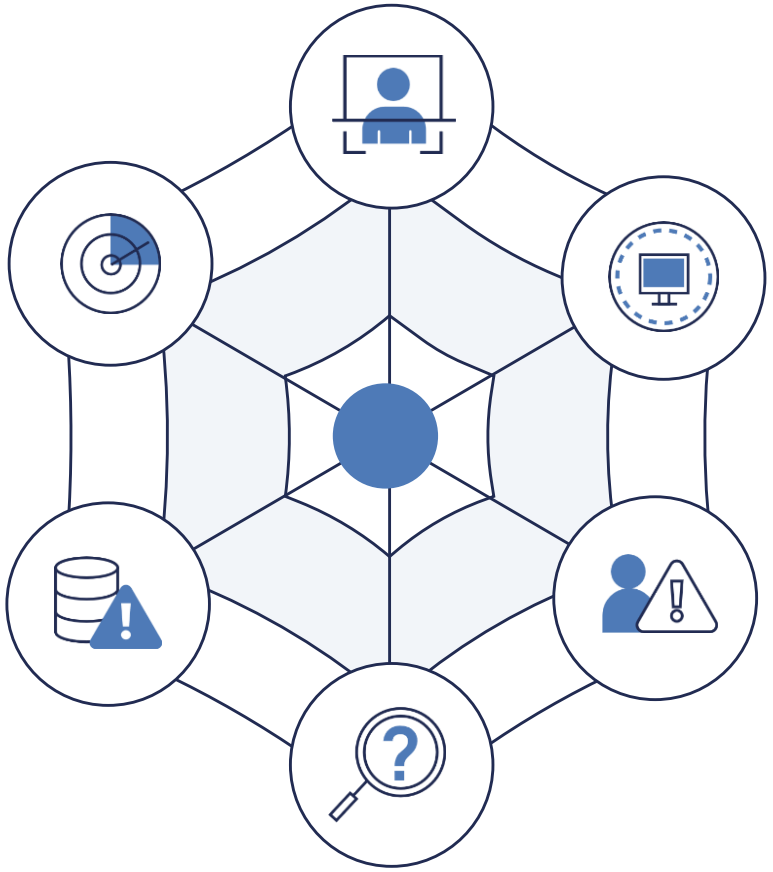
**Сложно отличить** от реальной инфраструктуры

Размещение и управление из **единого центра**, готовые шаблоны ловушек и приманок

# Когда нужен R-Vision TDP

Есть риск наличия в периметре внешнего
или внутреннего нарушителя

Необходимо вывести
обнаружение
угроз на новый уровень



Требуется дополнительный
слой защиты инфраструктуры

Есть специфические
и высококритичные активы

У сотрудников есть **прямой** доступ
к высококритичным ресурсам

Традиционные системы обнаружения
недостаточно эффективны

# Ключевые элементы R-Vision TDP

## Приманки

Информация, представляющая интерес для злоумышленника, которая приведет его в ловушку.

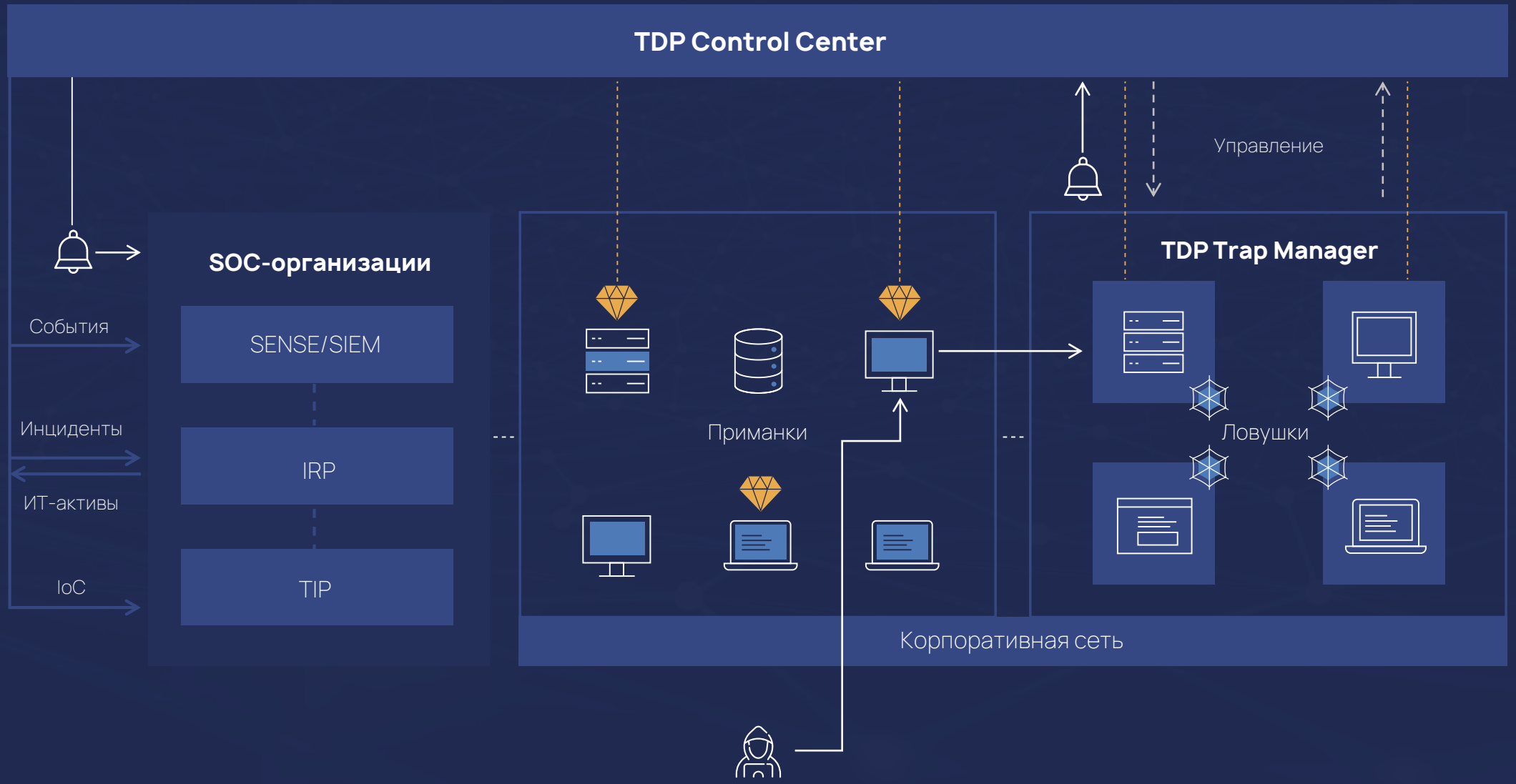
- Учетные записи
- Файлы данных
- История браузера
- Ключи и т. д.

## Ловушки

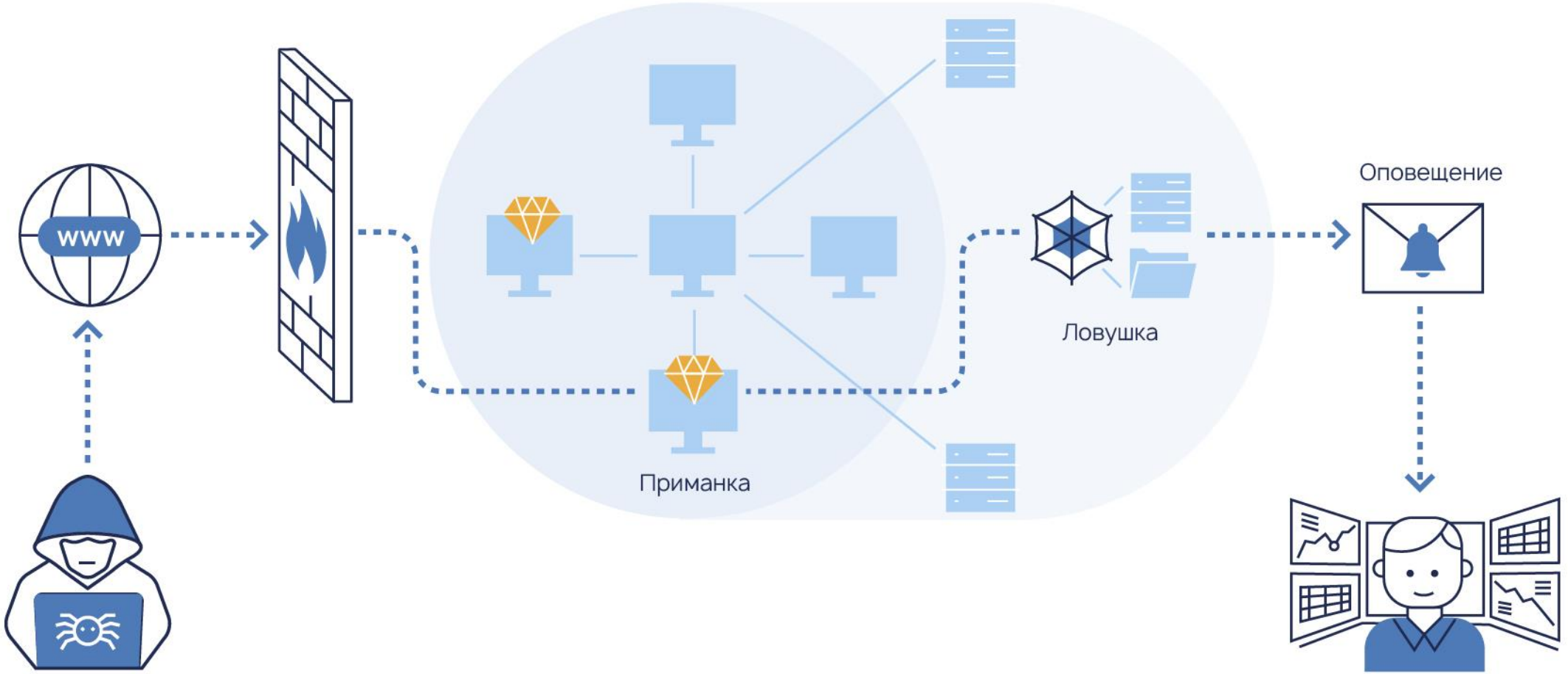
Ложные узлы сети, позволяющие обнаружить злоумышленника и отвлечь его от настоящих узлов.

- Рабочие станции
- Сетевое оборудование
- Серверы
- Сервисы и т. д.

# Состав R-Vision TDP

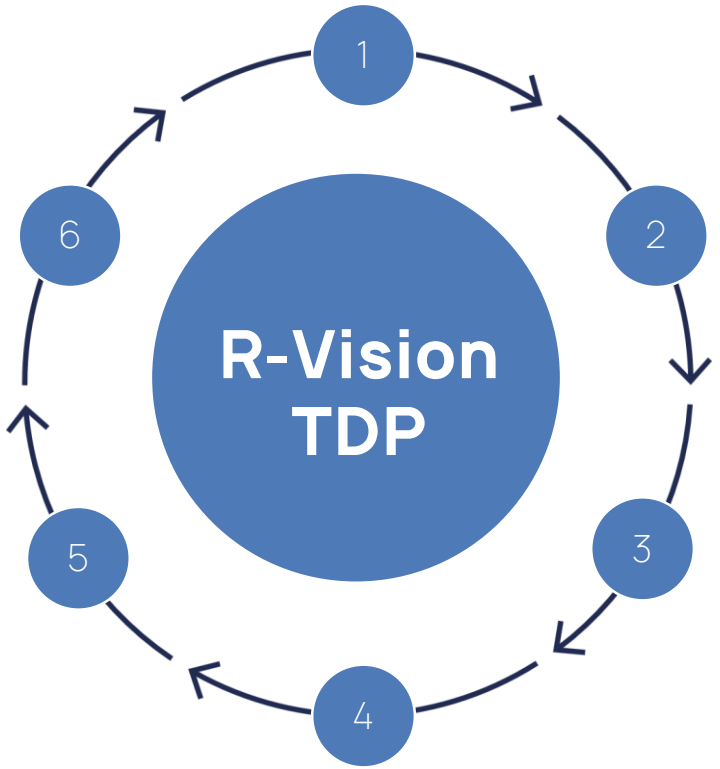


# Схема работы R-Vision TDP



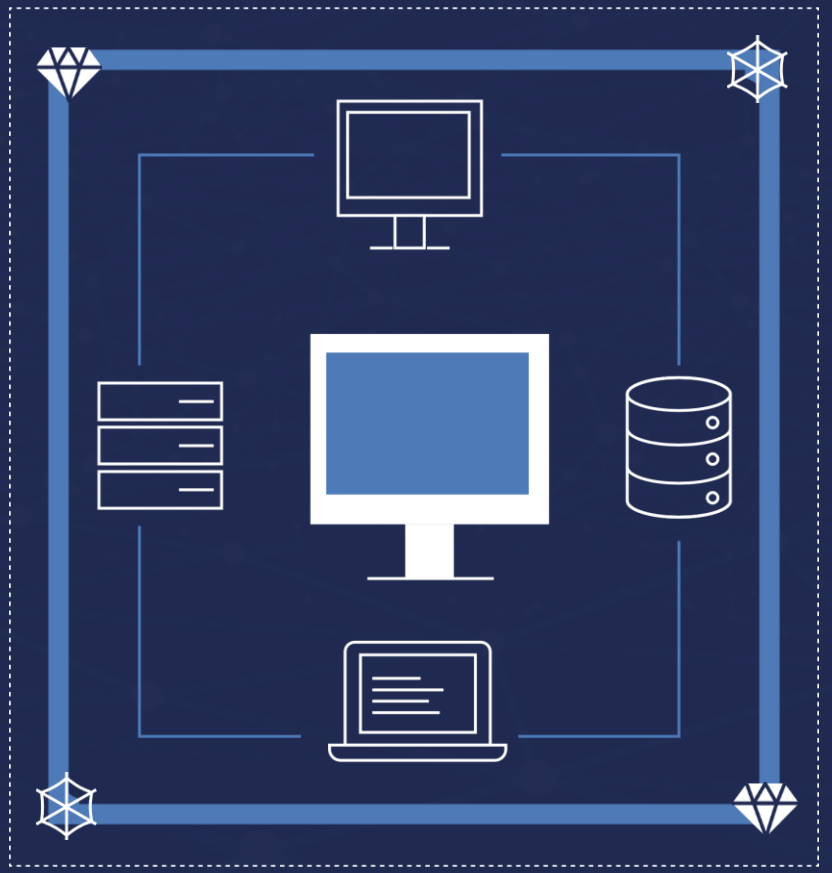
# Функции R-Vision TDP

1. Сбор данных об инфраструктуре для создания идеальной сети ловушек и приманок
2. Автоматическая генерация ловушек и приманок из шаблонов
3. Имитация любых систем, в том числе специфических
4. Автоматическая расстановка взаимосвязанных ловушек и приманок в инфраструктуре
5. Обнаружение злоумышленника, создание инцидентов и оповещение
6. Сбор данных и атрибутов атакующего для анализа



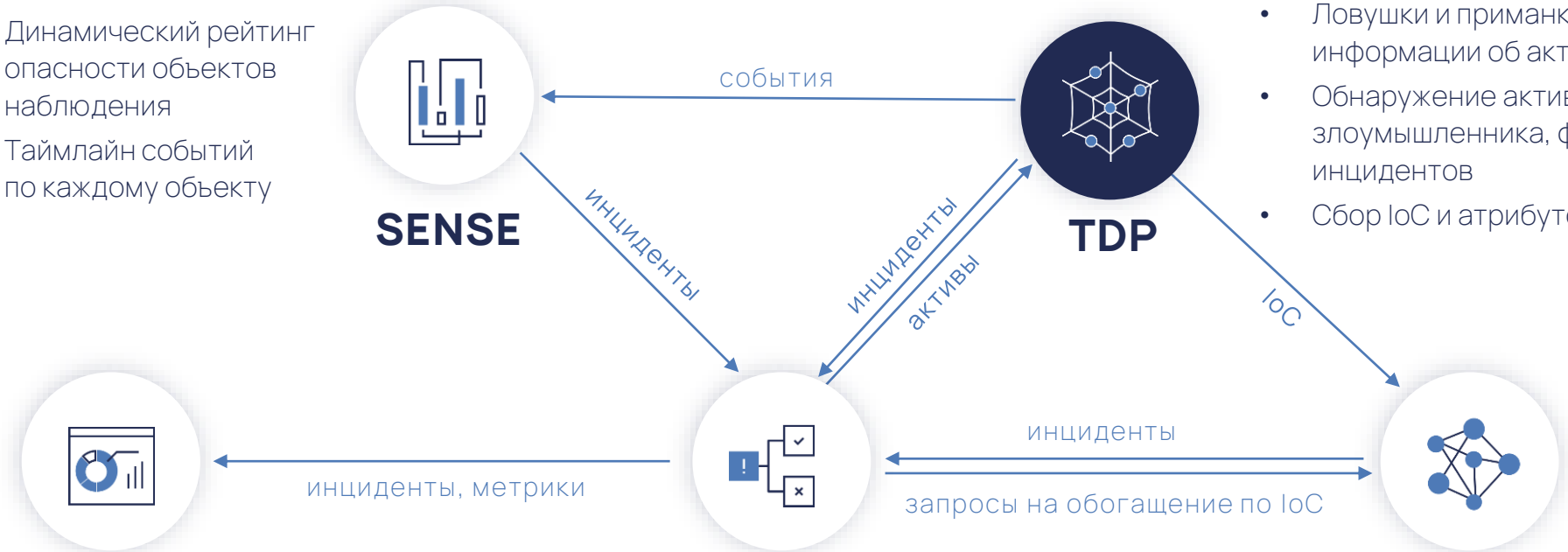
# Преимущества R-Vision TDP

- Широкий перечень видов ловушек и приманок
- Реалистичность для хакера за счет имитации системы с характерной деятельностью пользователей
- Безагентский способ работы снижает вероятность обнаружения злоумышленником
- Высокая скорость внедрения и масштабирования, автоматическое создание ловушек и приманок
- Выявление скомпрометированных систем и автоматизация реагирования в связке с другими продуктами R-Vision



# Место TDP в экосистеме R-Vision

- Динамический рейтинг опасности объектов наблюдения
- Таймлайн событий по каждому объекту

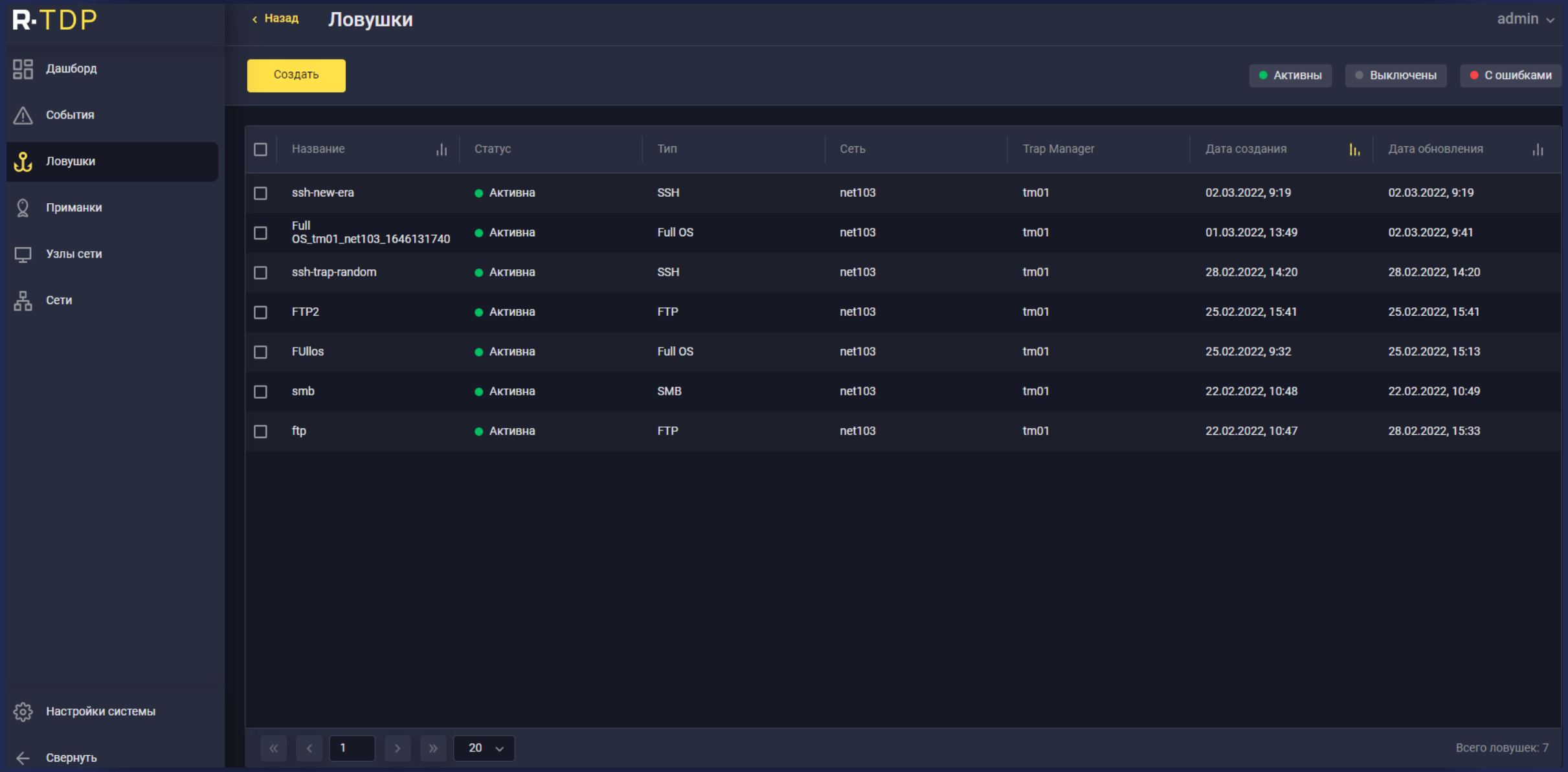



- Ловушки и приманки - на основе информации об активах
- Обнаружение активности злоумышленника, формирование инцидентов
- Сбор IoC и атрибутов атакующего

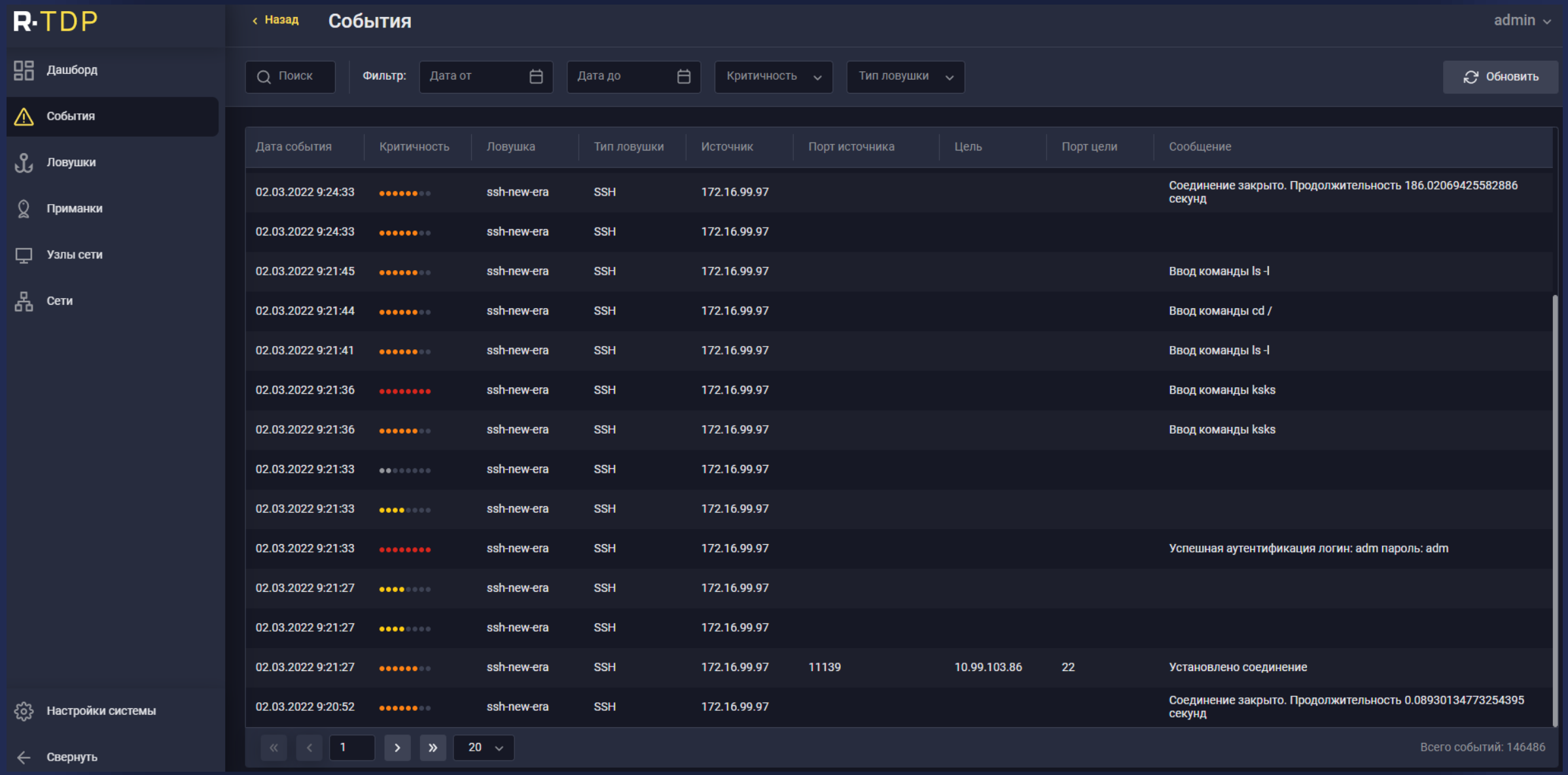
- Агрегация всей картины по ИБ
- Аудиты с ретроспективой
- Риски с учётом инцидентов

- Оркестрация
- Обмен с ФинЦЕРТ и ГосСОПКА
- Уязвимости с приоритизацией

- Экспорт IoC на СЗИ


R-TDP
Назад
Ловушки
admin
Дашборд
События
Ловушки
Приманки
Узлы сети
Сети
Настройки системы
Свернуть
Создать
Активны
Выключены
С ошибками
Название
Статус
Тип
Сеть
Trap Manager
Дата создания
Дата обновления
ssh-new-era Активна SSH net103 tm01 02.03.2022, 9:19 02.03.2022, 9:19
Full OS_tm01_net103_1646131740 Активна Full OS net103 tm01 01.03.2022, 13:49 02.03.2022, 9:41
ssh-trap-random Активна SSH net103 tm01 28.02.2022, 14:20 28.02.2022, 14:20
FTP2 Активна FTP net103 tm01 25.02.2022, 15:41 25.02.2022, 15:41
FUllos Активна Full OS net103 tm01 25.02.2022, 9:32 25.02.2022, 15:13
smb Активна SMB net103 tm01 22.02.2022, 10:48 22.02.2022, 10:49
ftp Активна FTP net103 tm01 22.02.2022, 10:47 28.02.2022, 15:33
1
20
Всего ловушек: 7

Ловушки


R·TDP
Назад
События
admin
Дашборд
События
Ловушки
Приманки
Узлы сети
Сети
Настройки системы
Свернуть
Поиск
Фильтр:
Дата от
Дата до
Критичность
Тип ловушки
Обновить
Дата события
Критичность
Ловушка
Тип ловушки
Источник
Порт источника
Цель
Порт цели
Сообщение
02.03.2022 9:24:33 ssh-new-era SSH 172.16.99.97 Соединение закрыто. Продолжительность 186.02069425582886 секунд
02.03.2022 9:24:33 ssh-new-era SSH 172.16.99.97
02.03.2022 9:21:45 ssh-new-era SSH 172.16.99.97 Ввод команды ls -l
02.03.2022 9:21:44 ssh-new-era SSH 172.16.99.97 Ввод команды cd /
02.03.2022 9:21:41 ssh-new-era SSH 172.16.99.97 Ввод команды ls -l
02.03.2022 9:21:36 ssh-new-era SSH 172.16.99.97 Ввод команды ksks
02.03.2022 9:21:36 ssh-new-era SSH 172.16.99.97 Ввод команды ksks
02.03.2022 9:21:33 ssh-new-era SSH 172.16.99.97
02.03.2022 9:21:33 ssh-new-era SSH 172.16.99.97
02.03.2022 9:21:33 ssh-new-era SSH 172.16.99.97 Успешная аутентификация логин: adm пароль: adm
02.03.2022 9:21:27 ssh-new-era SSH 172.16.99.97
02.03.2022 9:21:27 ssh-new-era SSH 172.16.99.97
02.03.2022 9:21:27 ssh-new-era SSH 172.16.99.97 11139 10.99.103.86 22 Установлено соединение
02.03.2022 9:20:52 ssh-new-era SSH 172.16.99.97 Соединение закрыто. Продолжительность 0.08930134773254395 секунд
1
20
Всего событий: 146486

События


R-TDP
Дашборд
События
Ловушки
Приманки
Узлы сети
Сети
Настройки системы
Свернуть
Назад
Дашборд
admin
За сегодня 3/2/2022
261
Количество событий
6
Количество ловушек в системе
00:06:58
Без происшествий
Топ 5 целей
IP адрес
Количество событий
10.99.103.110
126
10.99.103.117
114
10.99.103.86
3
События по типу ловушек
92 % Full OS
8 % SSH
События по критичности
32 % Критическая
35 % Средняя
33 % Низкая
<1 % Неизвестна
Количество событий за последние 24 часа
70
60
50
40
30
20
10
0
9:00 10:00 11:00 12:00 13:00 14:00 15:00 16:00 17:00 18:00 19:00 20:00 21:00 22:00 23:00 0:00 1:00 2:00 3:00 4:00 5:00 6:00 7:00 8:00 9:00
Последние 5 событий
09:31:21 Тип ловушки: Full OS
Special privileges assigned to new logon. Subject: Security ...
09:31:21 Тип ловушки: Full OS
Group membership information. Subject: Security ID: S-1-5-...
09:31:21 Тип ловушки: Full OS
An account was successfully logged on. Subject: Security I...
09:27:25 Тип ловушки: Full OS
Group membership information. Subject: Security ID: S-1-5-...
09:27:25 Тип ловушки: Full OS
Special privileges assigned to new logon. Subject: Security ...

Дашборд

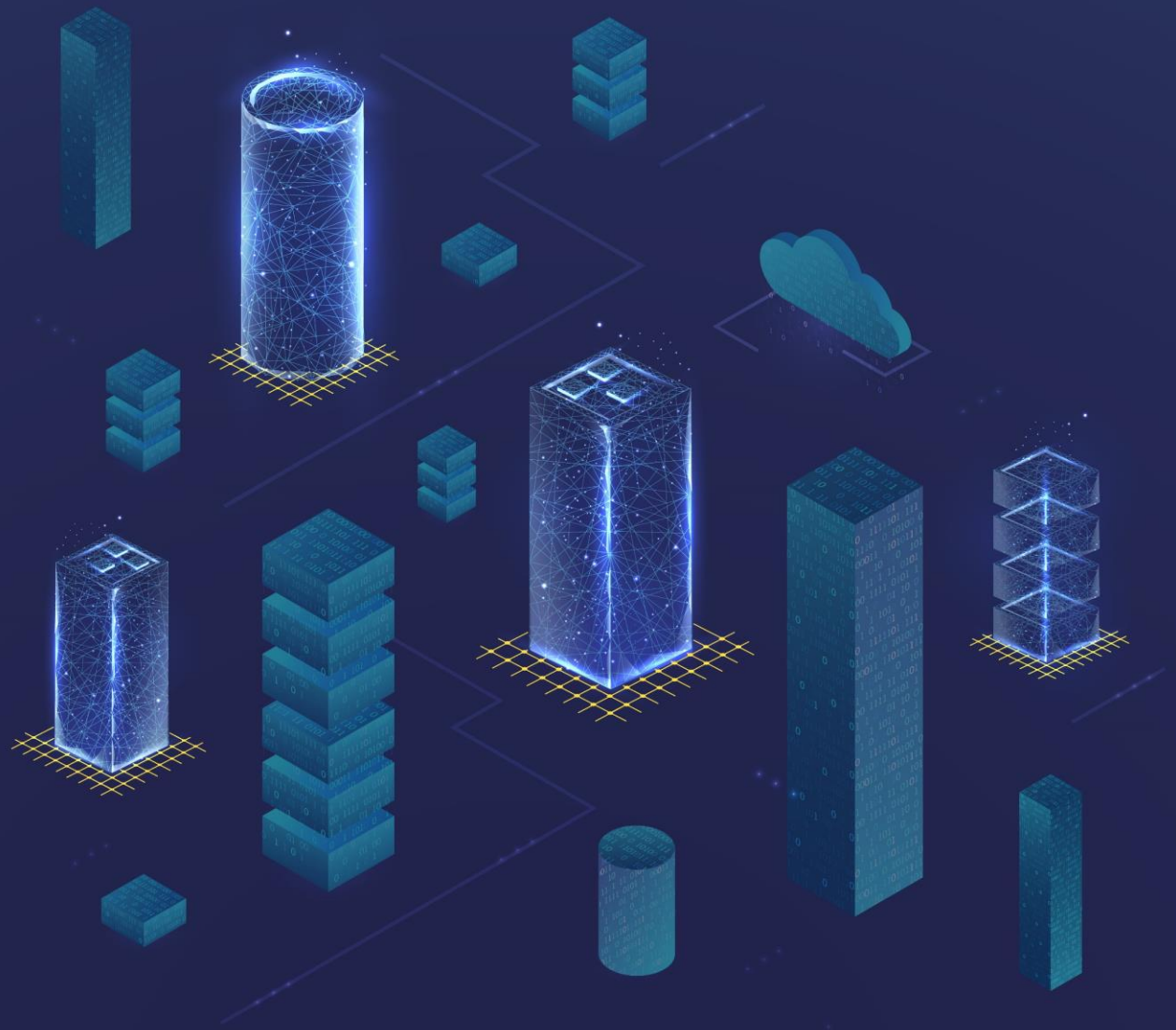
# Результат

**Обнаружение атак**, которые невозможно детектировать другими средствами (APT, 0-day и другие угрозы)

**Снижение скорости продвижения злоумышленника** внутри сети за счет созданного дополнительного слоя из эмулированных элементов

**Выявление слабых мест в защите**, понимание инструментов и действий атакующего в отношении инфраструктуры организации

**Возможность предотвратить атаки** до нанесения значительного ущерба



R-Vision

+ 7 (499) 322 80 40

sales@rvision.ru

www.rvision.ru

Подписывайтесь на наш дайджест ИБ: **rvision.ru/blog**