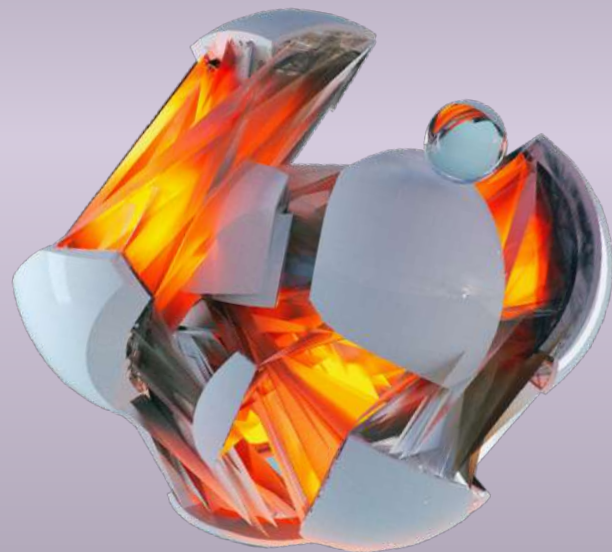


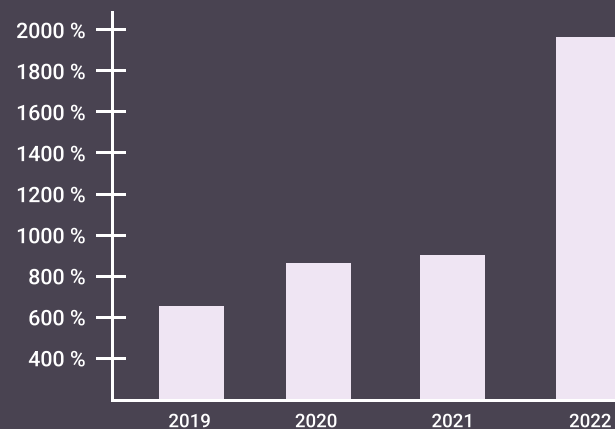


СИСТЕМА ЗАЩИТЫ ОТ
КИБЕРАТАК НА БАЗЕ
ТЕХНОЛОГИИ
DECEPTION

ПРОБЛЕМА



Вредоносные кампании, в ходе которых злоумышленники атакуют АСУ ТП, за год увеличились на 2000%. Это самая крупная цифра за последние три года.



Любое устройство в ИТ-инфраструктуре подвергается кибератакам

Атаки на цепочку поставок посредством подписанных официальным вендором обновлений

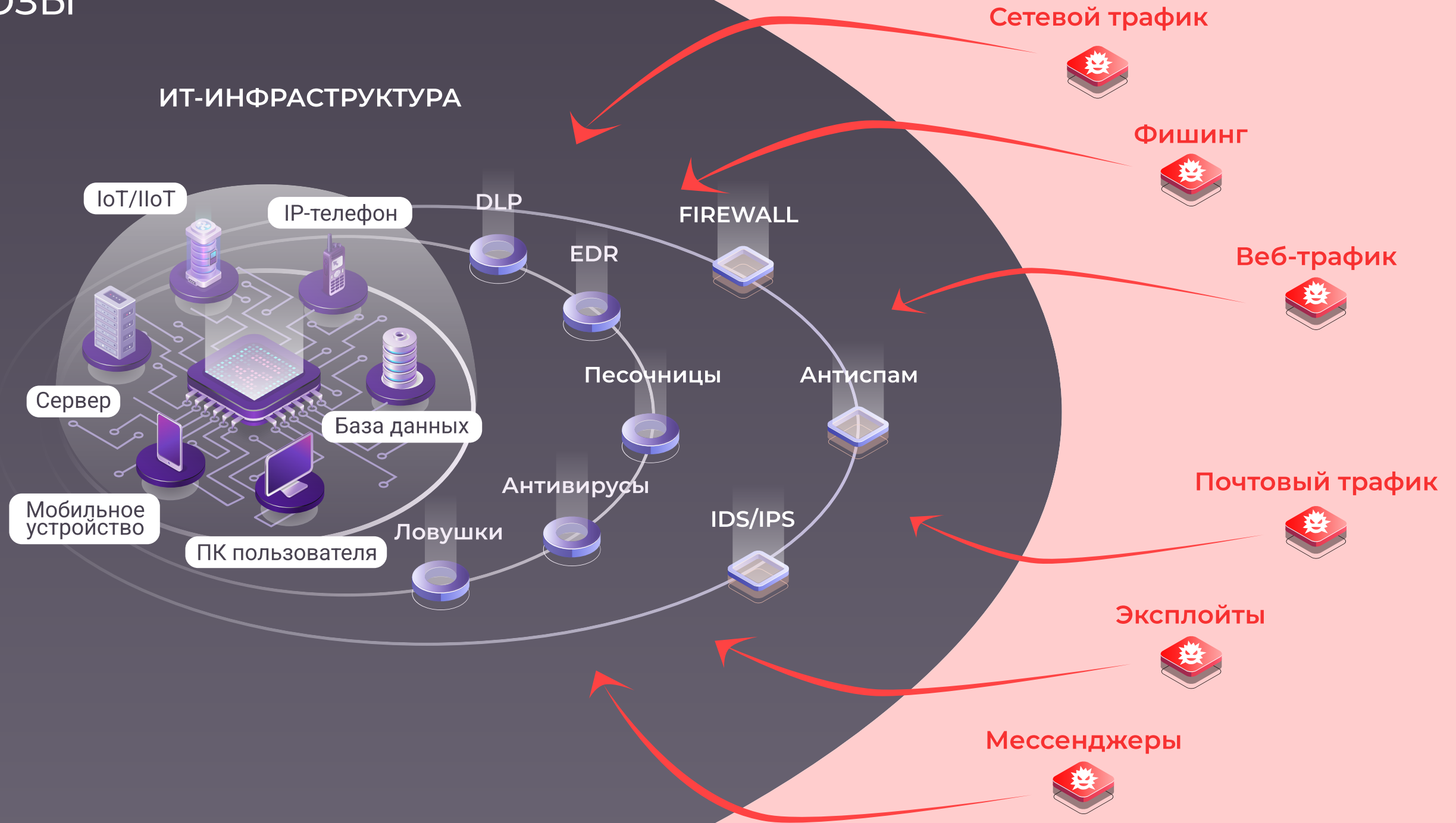
Атаки на IoT/IIoT, для которого слабо развита индустрия решений защиты и они имеют стандартные учетные данные

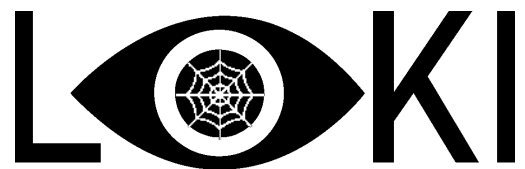
Внешние устройства, которые могут быть ошибочно проверены EDR решениями и агентами

Кибератаки, которые уже есть внутри организации

Сегментация с нулевым доверием, когда исключается доверие к любому инструменту защиты в организации, что подразумевает предположение о присутствии внешних и внутренних угроз

УГРОЗЫ





Система защиты от
целенаправленных атак на базе
технологии Deception

Запись в реестре отечественного
программного обеспечения
№11743 от 15.10.2021

ЕДИНАЯ ПАНЕЛЬ МОНИТОРИНГА И МЕНЕДЖМЕНТА

Приманка

Рабочее место
пользователя



- Логины и пароли
- Сессии посещения
- Подложные пользователи

Ловушка

Типы

- 1 Протоколы
- 2 Операционная система
- 3 Сервисы

Уровень интерактивности

Низкоинтерактивные



Среднеинтерактивные



Высокоинтерактивные

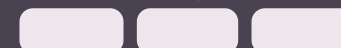


СХЕМА РАБОТЫ

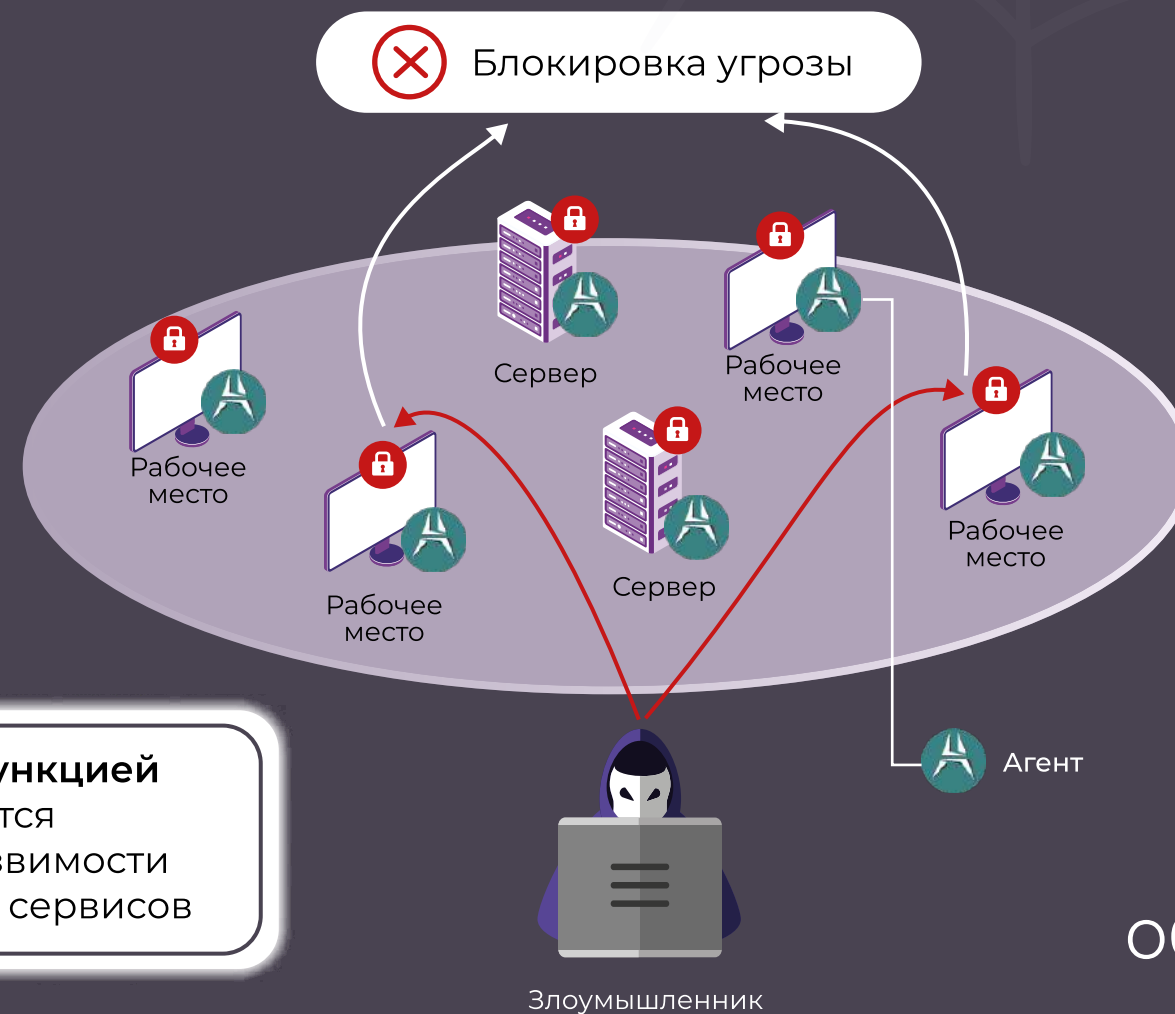


НАЗНАЧЕНИЕ СИСТЕМЫ

Основная задача системы - привлечь злоумышленника к ловушкам и приманкам, чтобы оповещать о кибератаках и оберегать реальные сервисы организации

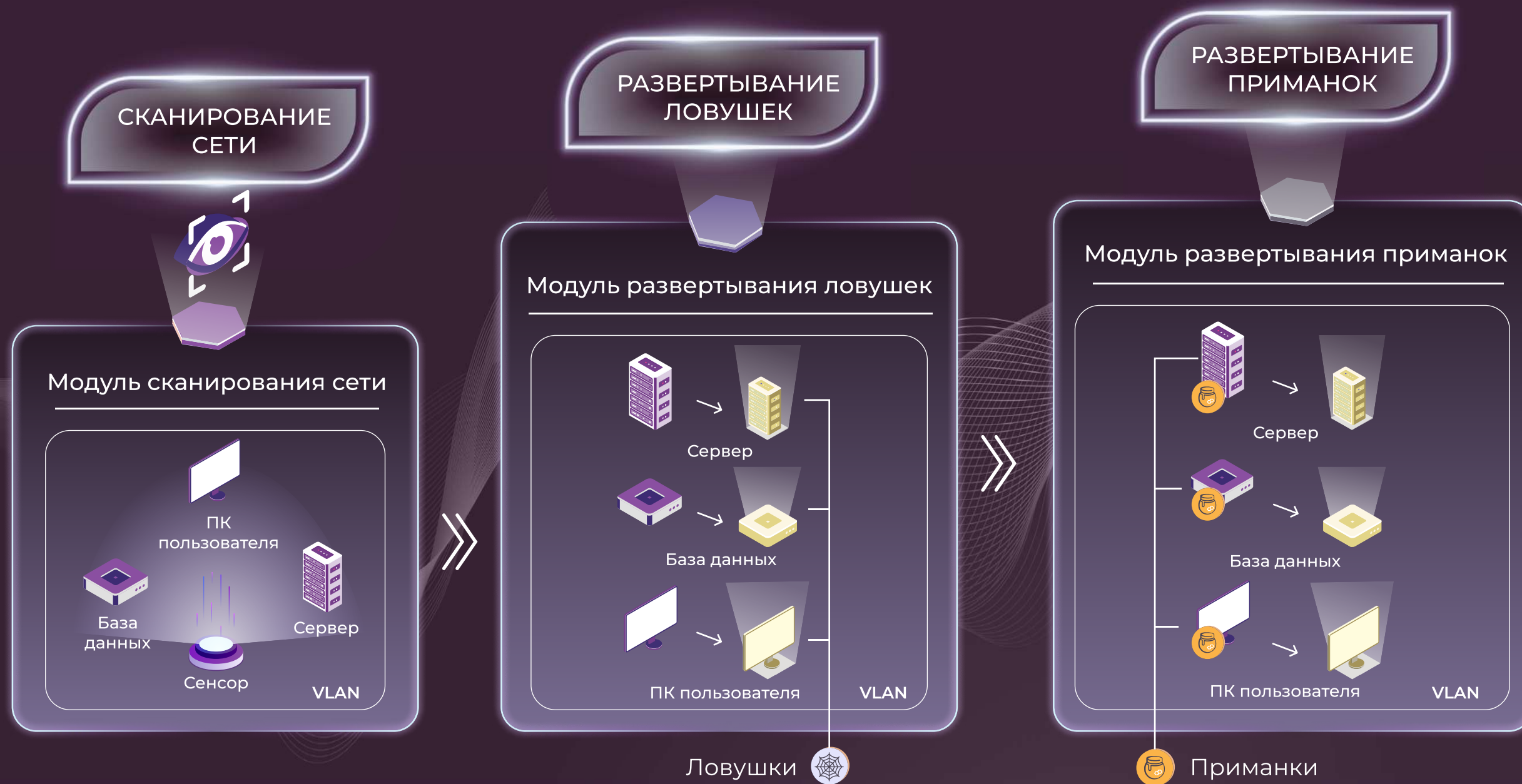


В системе присутствует режим блокировки распространения угрозы в подсети (VLAN). Блокировка осуществляется с помощью специальных агентов



Дополнительной функцией системы является сканирование на уязвимости реальных устройств и сервисов

РАЗВЕРТЫВАНИЕ



СЕНСОРЫ

Сенсоры располагаются в подсетях (VLAN), они осуществляют сканирование и развертывание ловушек.

По каждому сенсору в системе можно получить следующую информацию:



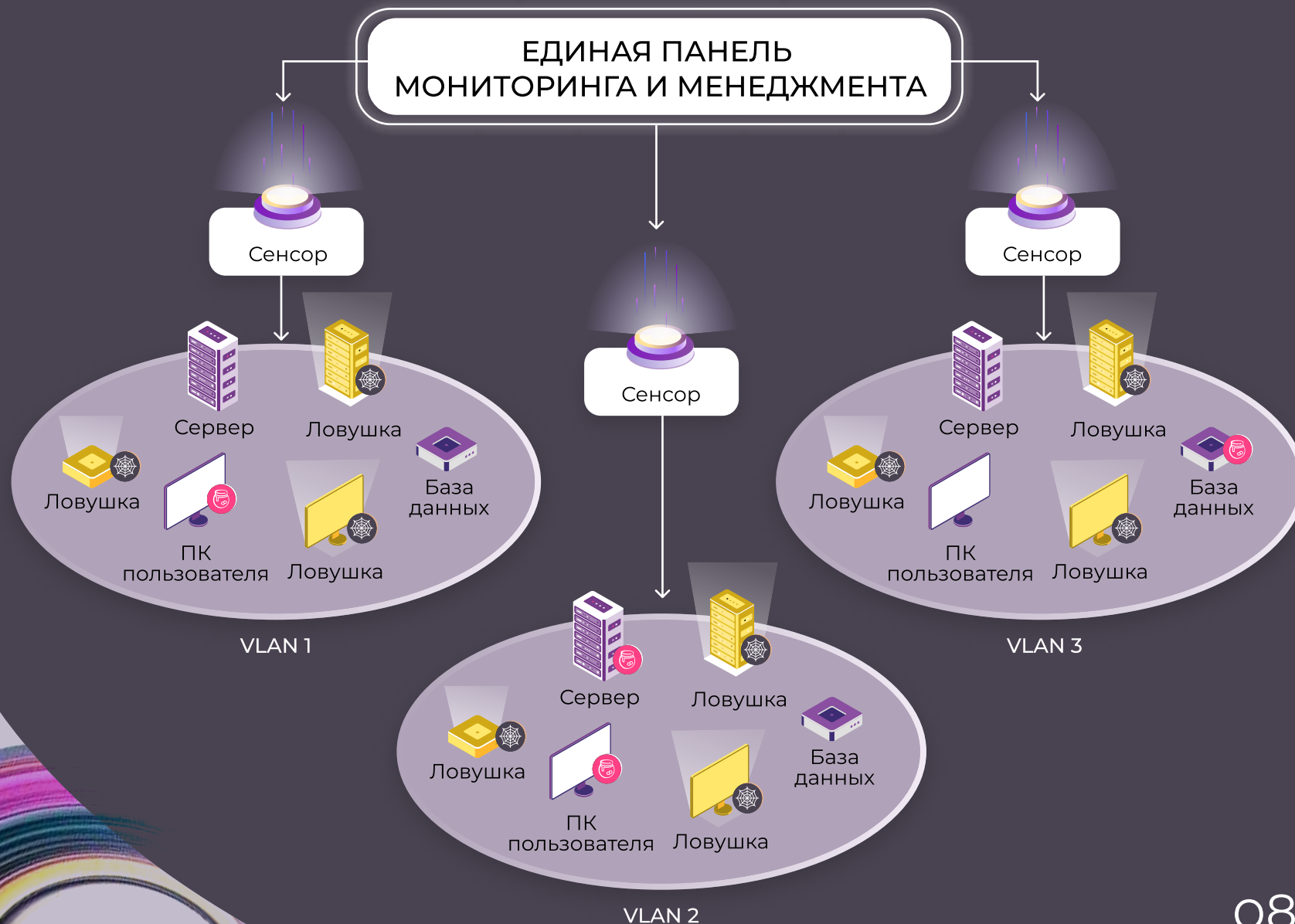
Ловушки, которые установлены в подсети



Приманки на рабочие места пользователей



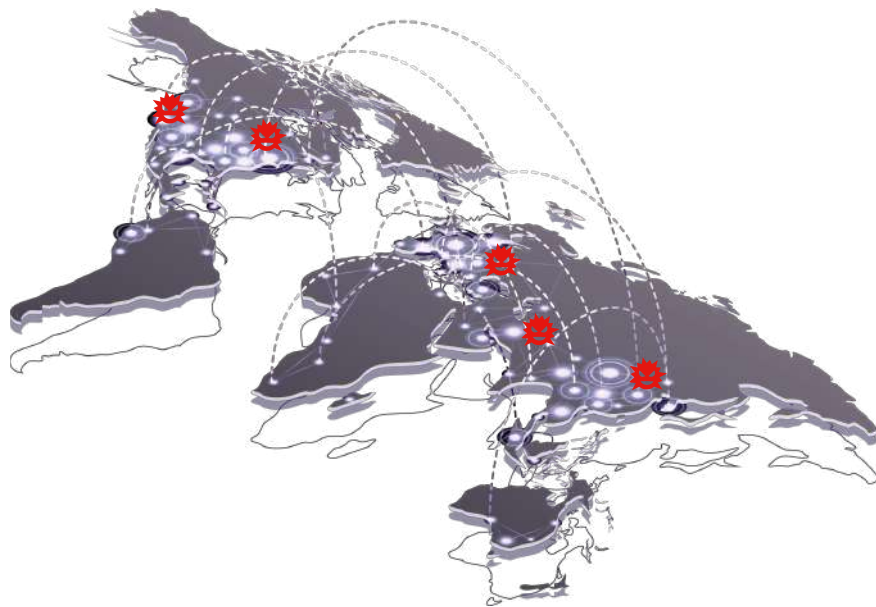
Устройства, которые были зафиксированы на момент крайнего сканирования



ТИПЫ ЛОВУШЕК

Исследовательские

Целью является получение как можно большего количества информации о кибератаках. Данный вид ловушек располагается преимущественно в сети Интернет и испытывает высокую нагрузку.



Промышленные

Направлены на защиту ИТ-инфраструктуры организации и располагаются внутри нее, имитируя различные используемые в ней устройства. Имеют приманки на рабочие места.



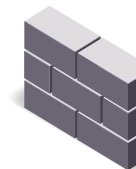
ПК Пользователя



Сервер



База данных



Межсетевой экран

ВИДЫ ЛОВУШЕК

Базы данных

- PostgreSQL
- MongoDB
- MySQL

Типы имитируемых устройств

- Межсетевые экраны
- SCADA
- IoT/IIoT
- Файловые сервера
- IP-телефония
- IP-камеры
- Станки
- Маршрутизаторы
- Коммутаторы
- Операционные системы
- Базы данных
- Рабочие места

Поддерживаемые протоколы

FTP, HTTP, HTTPS, SSH, RDP, IMAP, IMAPS, NTP, POP3, POP3S, SMB, SMTP, SNMP, SSL/TLS, TCP/UDP, DNS, TELNET, MODBUS TCP, IEC61850, OPC UA, S7COMM, SIP, BACNET, ENIP, IPMI, MSRPC, NETBIOS-SSN, TFTP, HC NET, RTSP, UPNP, LPD, WSDAPI

Генерация трафика между ловушками в целях маскировки

ПРИМАНКИ



Приманки обновляются каждые 24 часа, чтобы для злоумышленника быть актуальными для использования в процессе кибератаки



Генерация приманок осуществляется отдельно для каждой операционной системы, на текущий момент это Windows и Linux



Все приманки подходят к ловушкам в рамках своей подсети

ЕДИНАЯ ПАНЕЛЬ МОНИТОРИНГА И МЕНЕДЖМЕНТА

Приманка

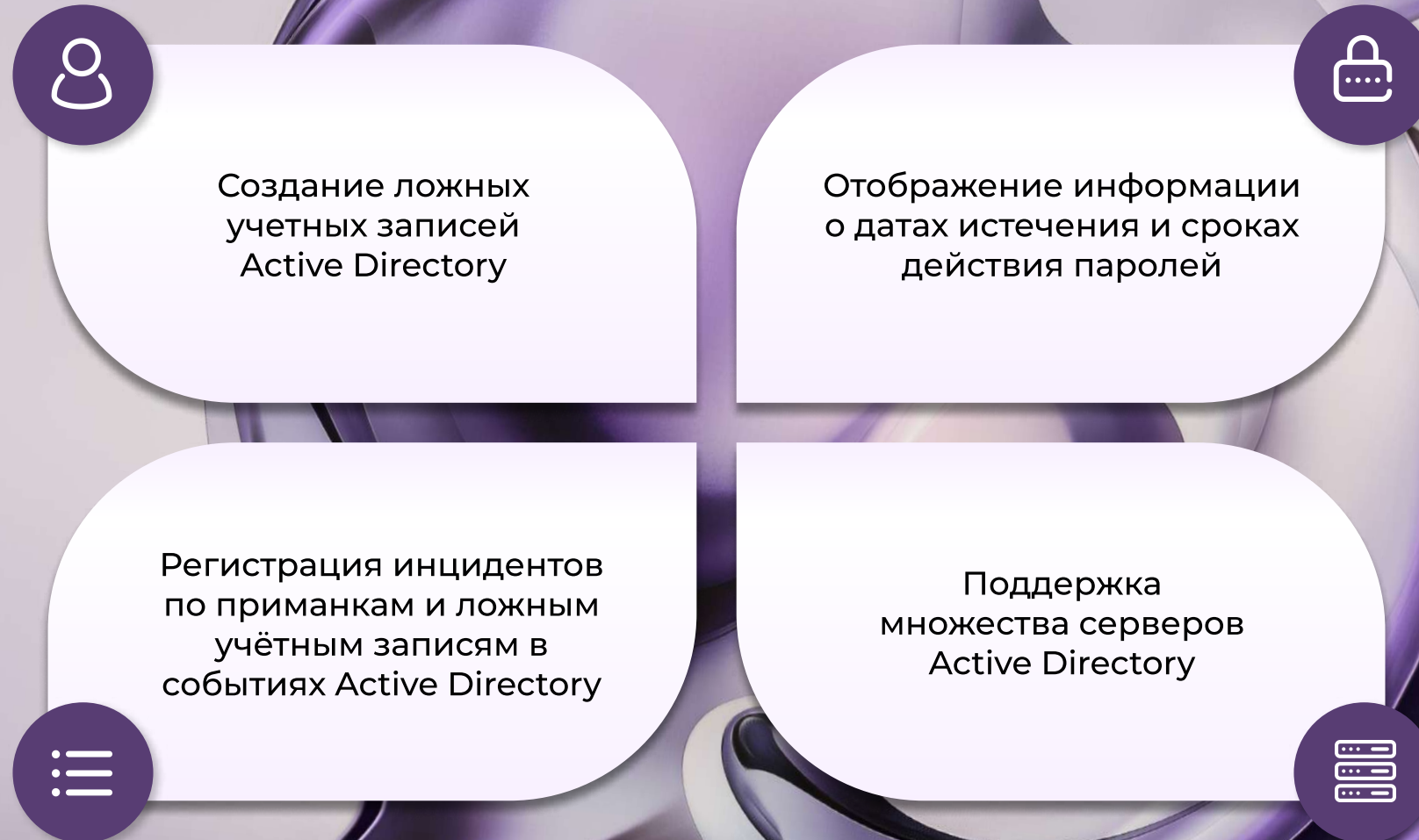
Рабочее место
пользователя



- Логины и пароли
- Сессии посещения
- Подложные пользователи
- Шаблонизация параметров

Приманки можно
распространить агентным
и безагентным способом

ACTIVE DIRECTORY



Отчет по сетевой атаке № 537613

Подобная информация

20.03.2023

09:15:43

192.168.8.1

Ловушка

Сенсор

ID

Время атаки

Протоколы

nginx_server

loki-sensor-dev

537613

00:00:01

http

Домен

FQDN Ловушки

Адрес ловушки

FQDN Атакующего

Адрес атакующего

-

nginx-2

192.168.8.23

-

192.168.8.1

События

Атаки в сессии

Файлы

Карта атак

Suricata

Время

Протокол

Действие

Событие

Комментарий

Ложное

Действия

06:15:42.725

http

Подключение

Подключение 192.168.8.1:48343 -> 192.168.8.28:80

06:15:42.725

http

Запрос

URL: /
Метод: GET

06:15:42.727

http

Запрос

URL: /favicon.ico
Метод: GET

06:15:42.727

http

Отключение

Отключение

06:15:45.633

http

Запрос

URL: /
Метод: GET

06:15:46.535

http

Запрос

URL: /
Метод: GET

06:15:46.535

http

Отключение

Отключение

1 из 1

10



Подробная информация по атаке



Схема перемещения атаки по сети



Получение полного списка команд и файлов



Справочники вредоносных IP-адресов и доменов



Интеграция с внешними аналитическими источниками



Интенсивность и общее время длительности кибератаки

СКАНИРОВАНИЕ НА УЯЗВИМОСТИ

Система LOKI осуществляет сканирование на уязвимости сервисы организации



Сканирование TCP/UDP портов



Сканирование белых IP-адресов



Обнаружение уязвимостей в сервисах:

- SMB
- HTTP
- FTP
- RDP
- SNMP
- SSM

- Привязка к CVE
- Указание хостов
- Ранжирование важности
- Сканирование по расписанию

Сканирование уязвимостей

- ОС Windows, Linux, Unix
- Сетевое оборудование
- Систем виртуализации
- Веб-серверов
- Веб-приложений и их серверов
- ERP-систем

ПРЕИМУЩЕСТВА



Поддержка большого количества типов ловушек и протоколов, в том числе IoT-устройств и технологического оборудования (АСУ ТП)



Интеграция с Suricata для выявления вредоносных сигнатур при атаках на ловушки



Использование как без агентской, так и агентской архитектуры для работы без прав доменного или локального администратора



Возможность блокировки обнаруженных атак и распространения вредоносного ПО в сети организации



Возможность периодического (по расписанию) сканирования рабочих мест, серверов и оборудования на известные уязвимости



Интеграция с песочницами Windows/Linux, включая отечественные ОС



Возможность кастомизации ловушек

КОНТАКТЫ

Спасибо, что нашли
время ознакомиться
с презентацией!



+7 (495) 988-92-25



office@avsw.ru



127106, г. Москва,
ул. Гостиничная, д.5



www.avsw.ru