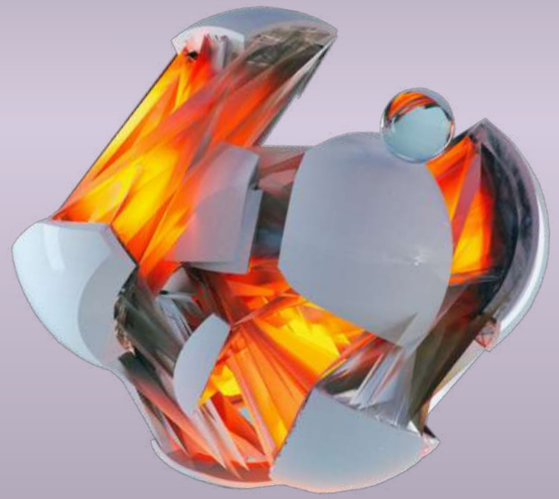
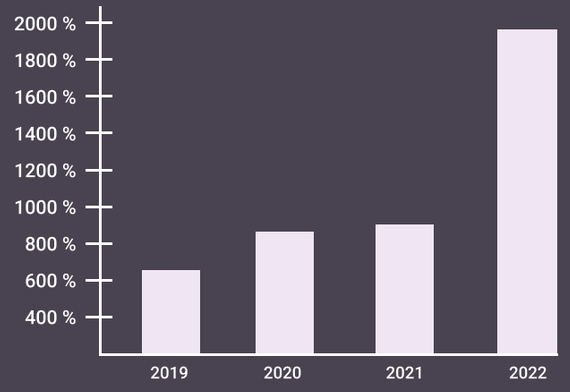

LOKI
СИСТЕМА ЗАЩИТЫ ОТ
КИБЕРАТАК НА БАЗЕ
ТЕХНОЛОГИИ
DECEPTION
AV SOFT

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

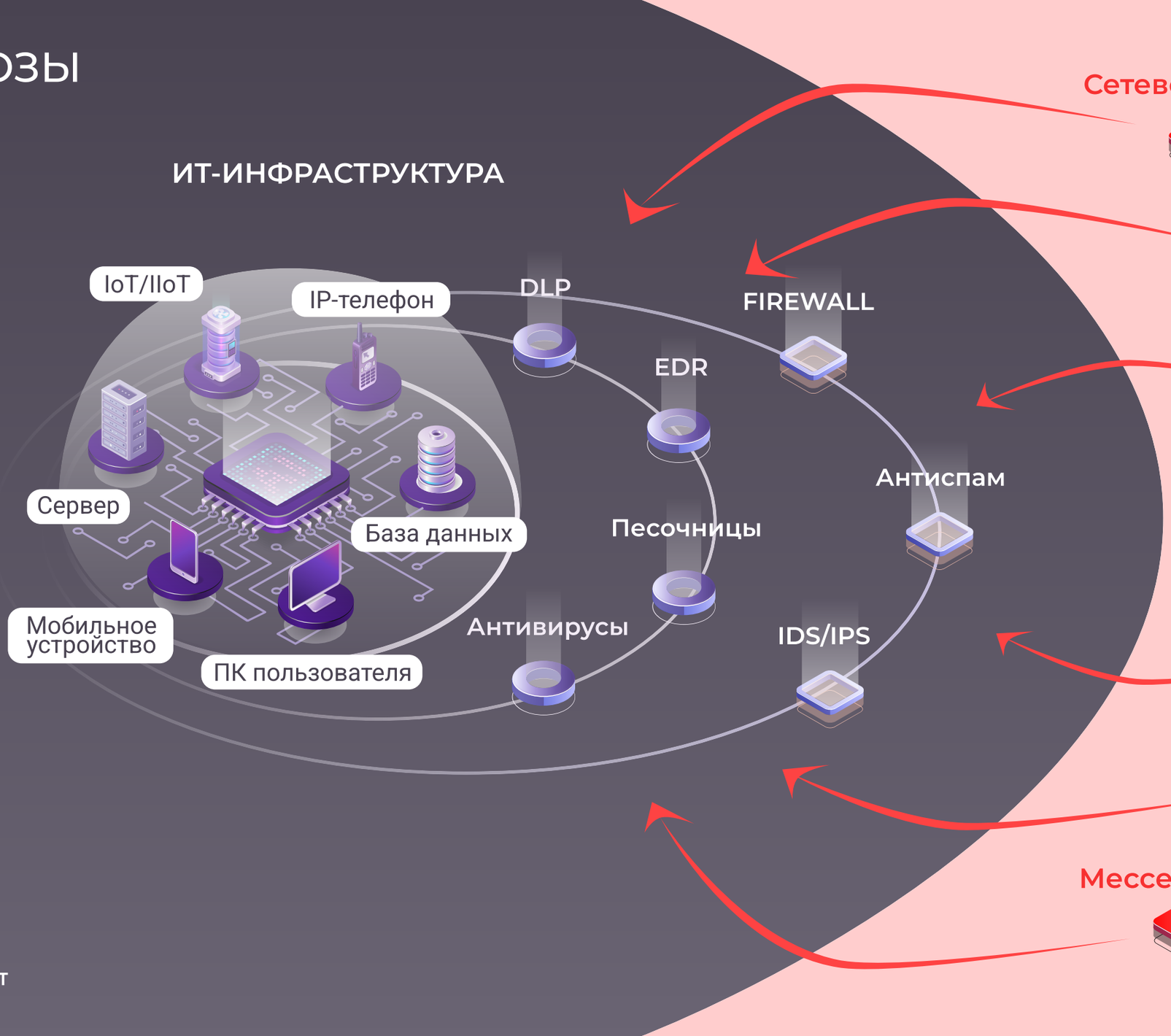
Атаки на IoT/IIoT, для которого слабо развита индустрия решений защиты и они имеют стандартные учетные данные

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


ИТ-ИНФРАСТРУКТУРА
IoT/IIoT
IP-телефон
Сервер
База данных
Мобильное устройство
ПК пользователя
DLP
EDR
Песочницы
Антивирусы
FIREWALL
Антиспам
IDS/IPS
Сетевой трафик
Фишинг
Веб-трафик
Почтовый трафик
Эксплойты
Мессенджеры

РЕШЕНИЕ

LOKI

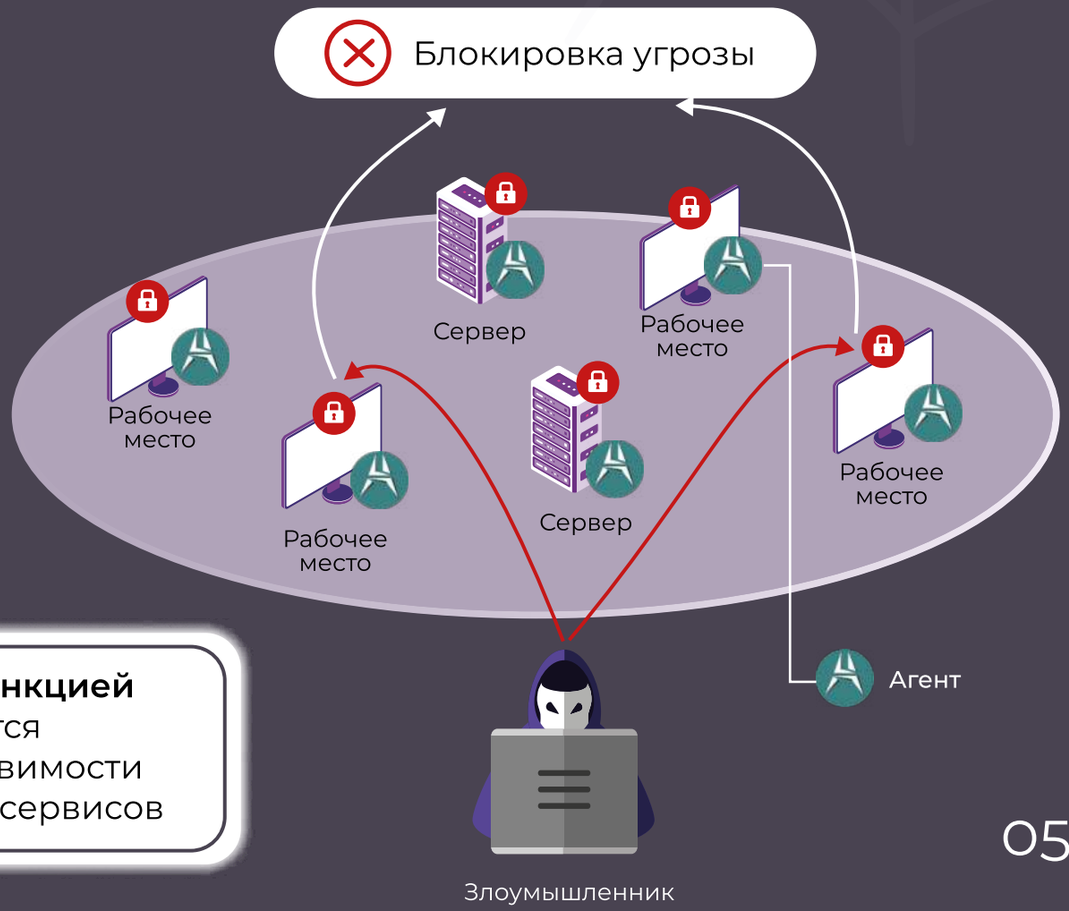
Система защиты от кибератак
на базе технологии Deception

Запись в реестре отечественного
программного обеспечения
№11743 от 15.10.2021

НАЗНАЧЕНИЕ СИСТЕМЫ

Основная задача системы - привлекать 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



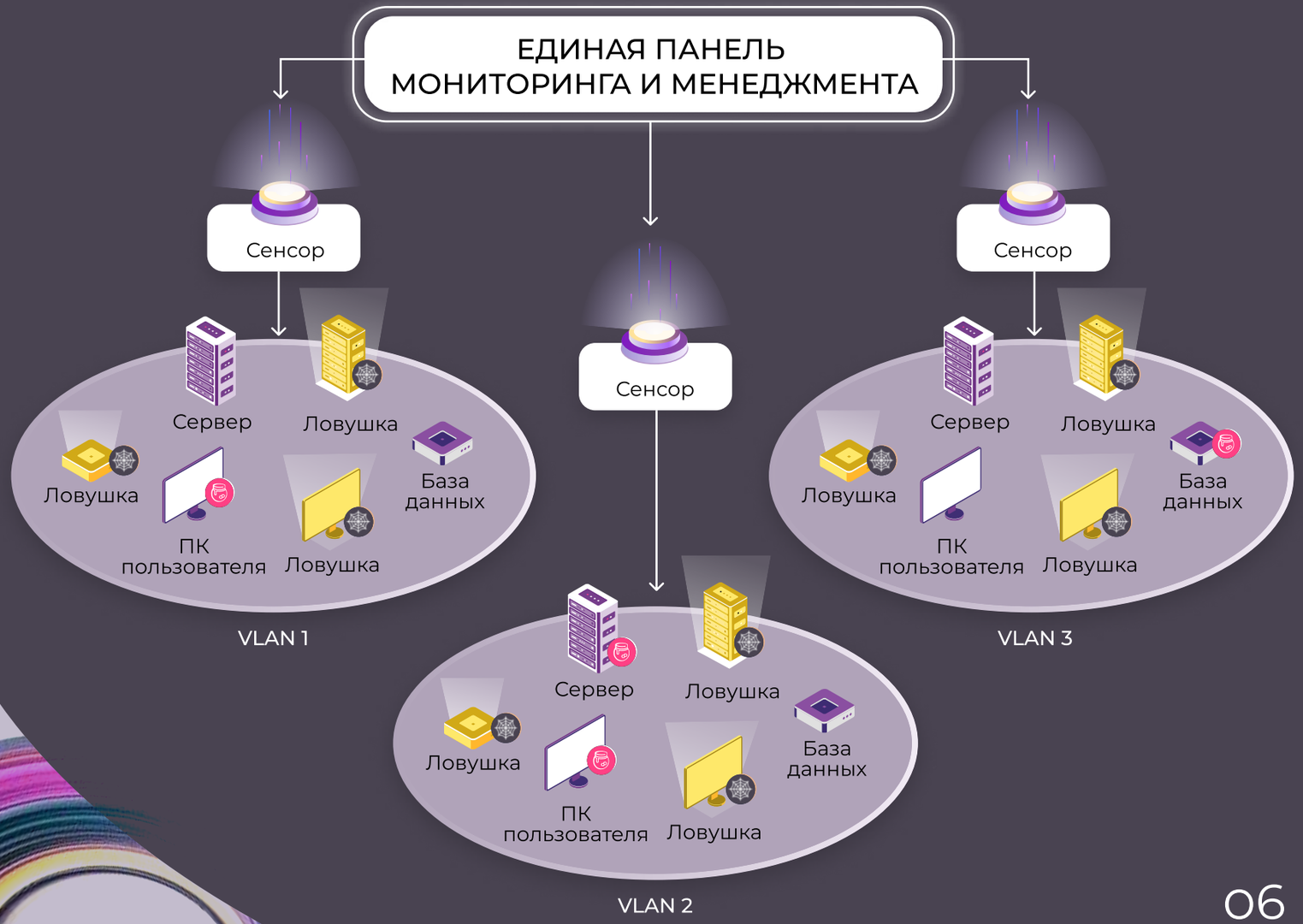
Дополнительной функцией системы является сканирование на уязвимости реальных устройств и сервисов

АРХИТЕКТУРА

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

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



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

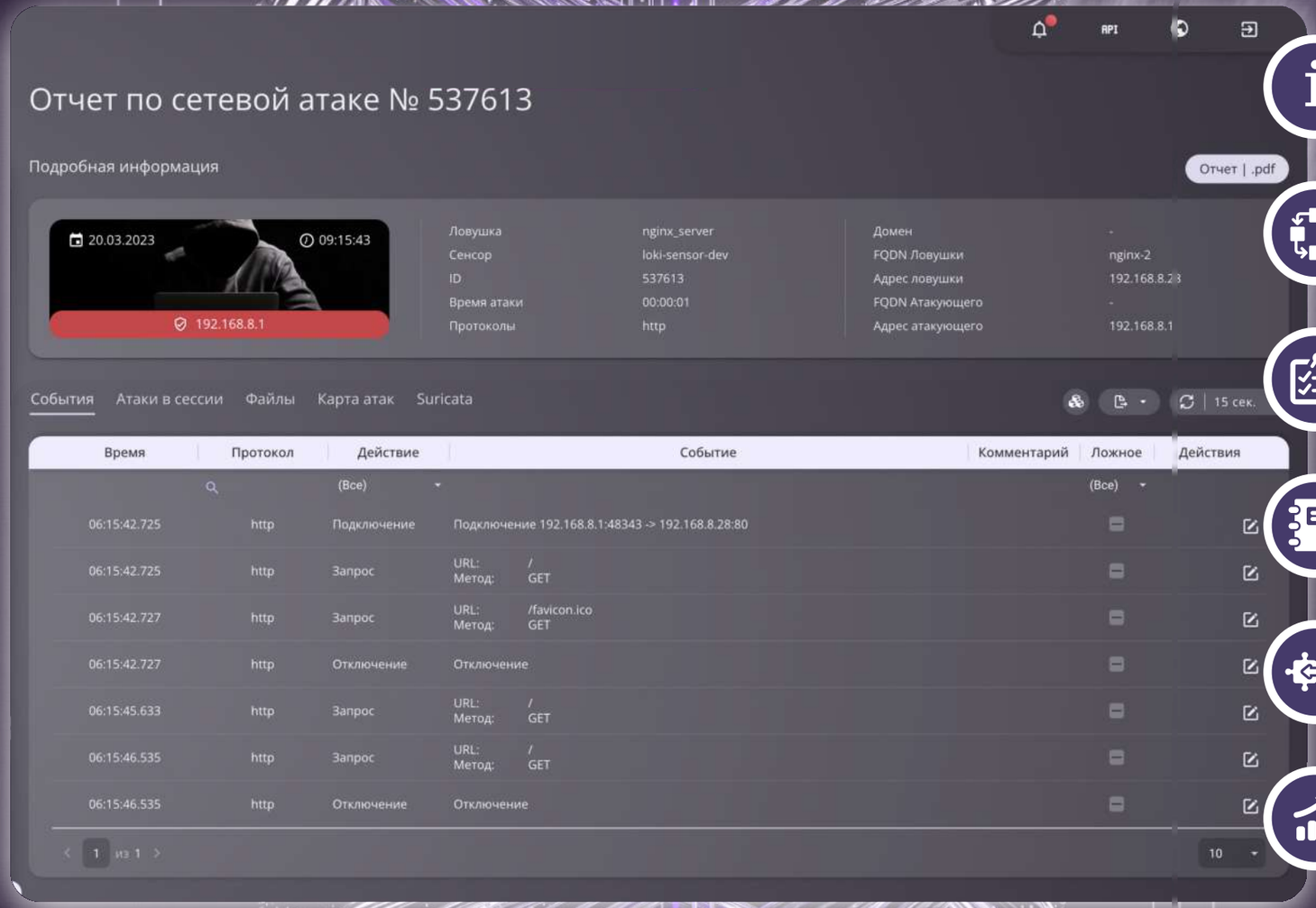
Генерация приманок осуществляться отдельно для каждой операционной системы, на текущий момент это Windows и Linux

Все приманки подходят к ловушкам в рамках своей подсети

РАЗВЕРТЫВАНИЕ

СХЕМА РАБОТЫ

ОТЧЕТ



- 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

ПРЕИМУЩЕСТВА

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

Шаблоны, конструкторы, возможность кастомизации ловушек и приманок

Поддержка большего 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

Маскировка ловушек и генерация трафика между ловушками

КОНТАКТЫ

Спасибо, что нашли
время ознакомиться
с презентацией!