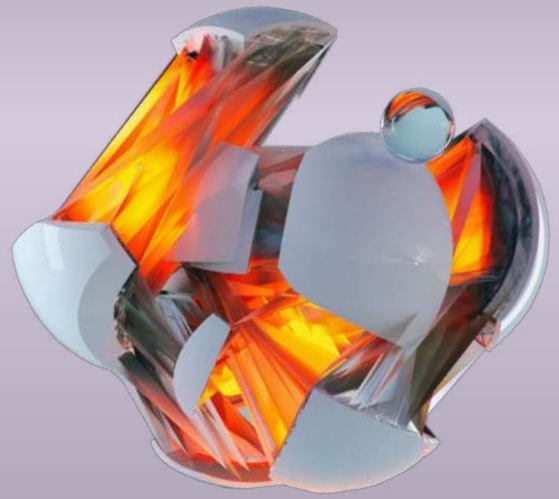
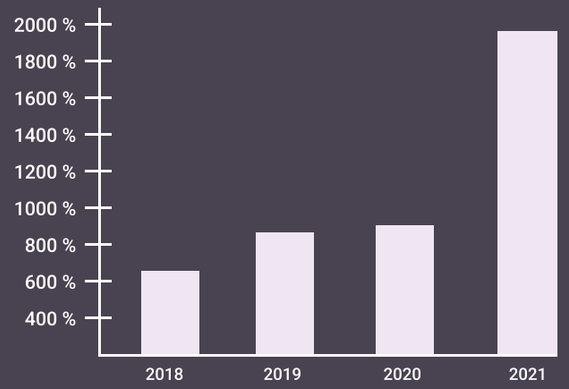

AV SOFT
LOKI
СИСТЕМА ЗАЩИТЫ ОТ КИБЕРАТАК НА БАЗЕ ТЕХНОЛОГИИ DECEPTION

ПРОБЛЕМА



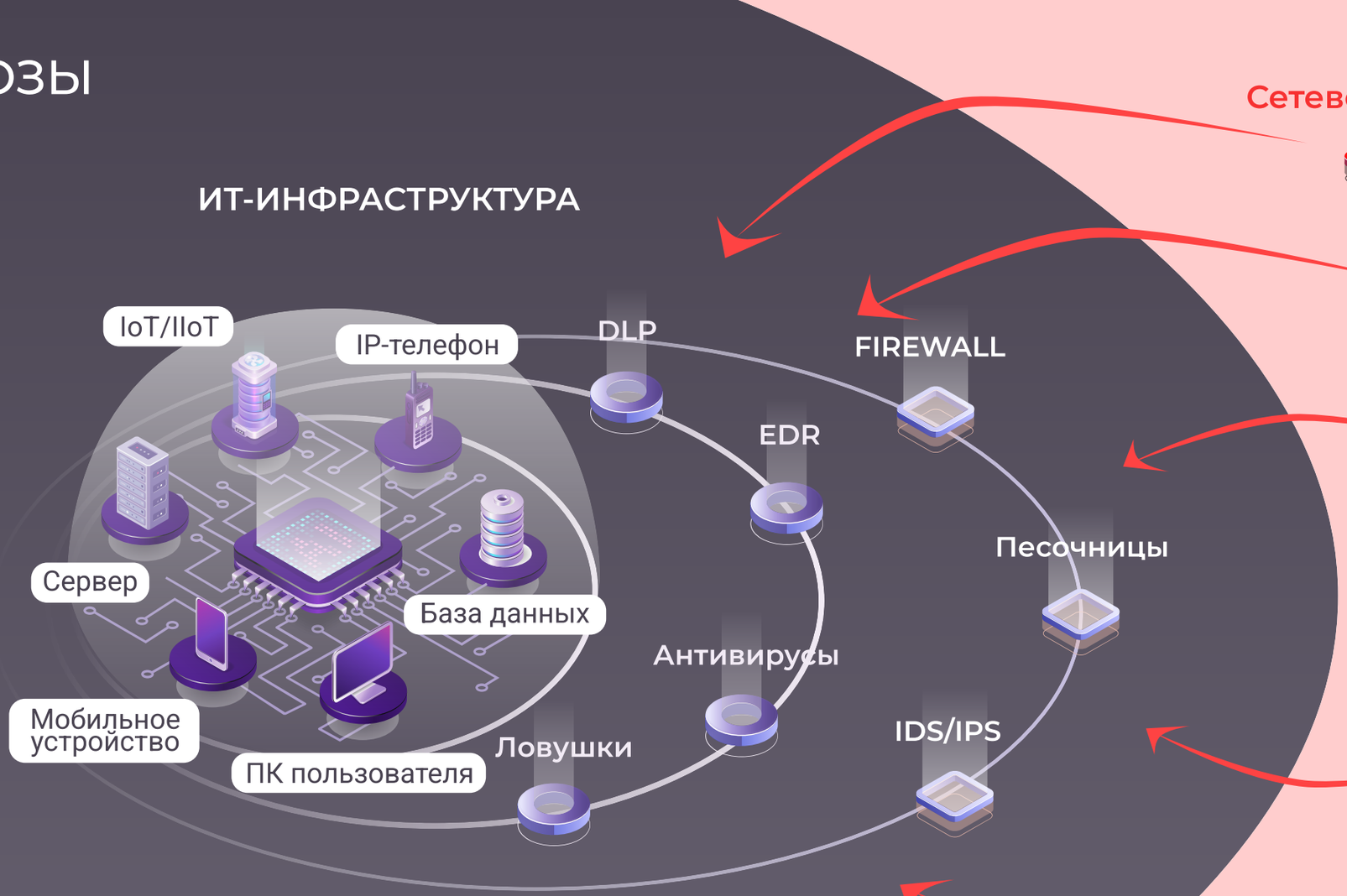
Вредоносные кампании, в ходе которых злоумышленники атакуют АСУ ТП, за год увеличились на 2000%. Это самая крупная цифра за последние три года.



Любое устройство в ИТ-инфраструктуре подвергается кибератакам

- Манипуляции с критическими бизнес-процессами
- Проникновения в корпоративную сеть и заражение устройств
- Преодоление всех периметров защиты
- Кибератаки, которые уже есть внутри
- Шифрование и уничтожение информационных активов

УГРОЗЫ



Сетевой трафик

Фишинг

Веб-трафик

Почтовый трафик

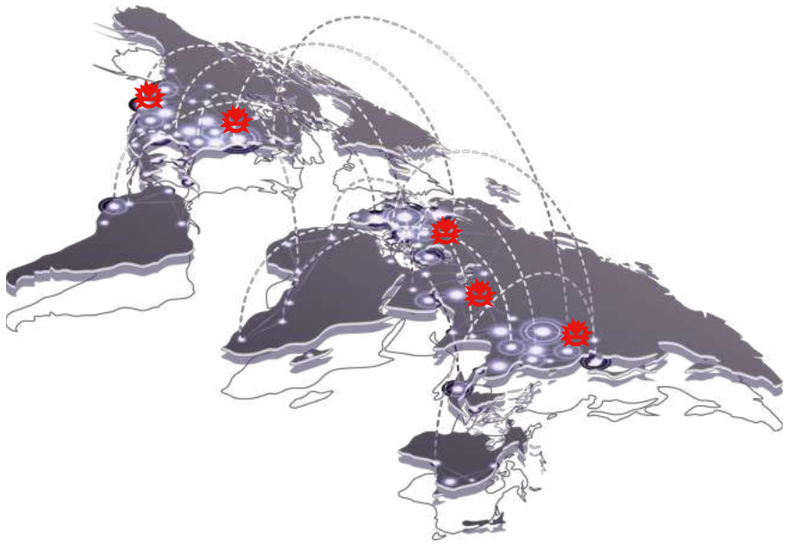
Эксплойты

Мессенджеры

ТИПЫ ЛОВУШЕК

Исследовательские

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



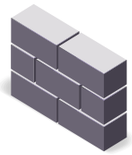
Промышленные

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

ПК Пользователя

Сервер

База данных



Межсетевой экран

РЕШЕНИЕ

LOKI

Система распределенных ложных целей для защиты ИТ инфраструктуры от внутренних и внешних угроз

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

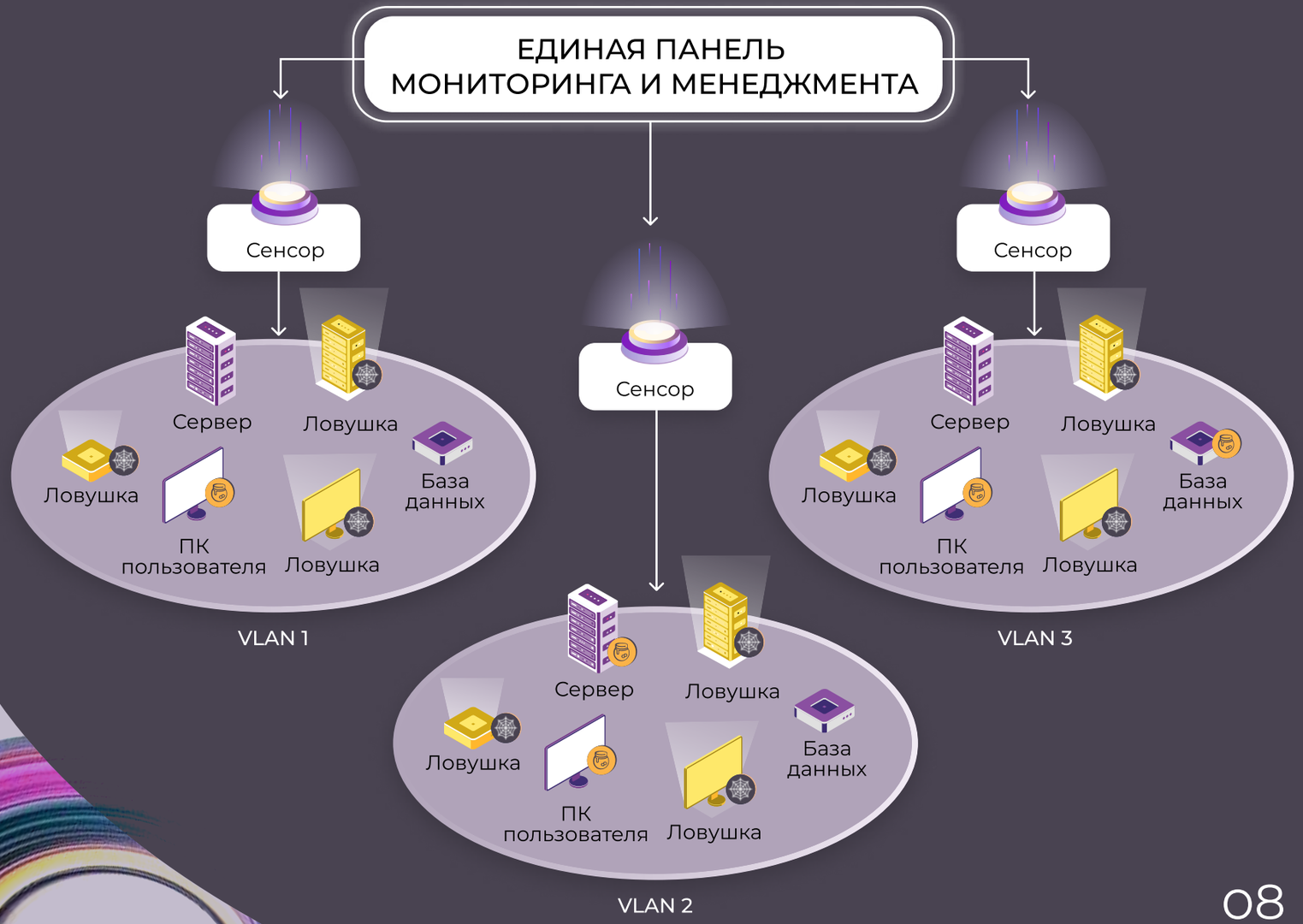
РАЗВЕРТЫВАНИЕ

СЕНСОРЫ

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

Типы имитируемых устройств

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

Поддерживаемые протоколы

FTP, gQUIC, HTTP, HTTPS, IMAP, IMAPS, NTP, POP3, POP3S, RDP, SMTP, SSH, SOCKS5, SSL/TLS, TCP/UDP, DNS, Telnet, Modbus TCP, IEC 104, OPC UA, IEC 61850 MMS, S7Comm

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

СХЕМА РАБОТЫ

КИБЕРАТАКА

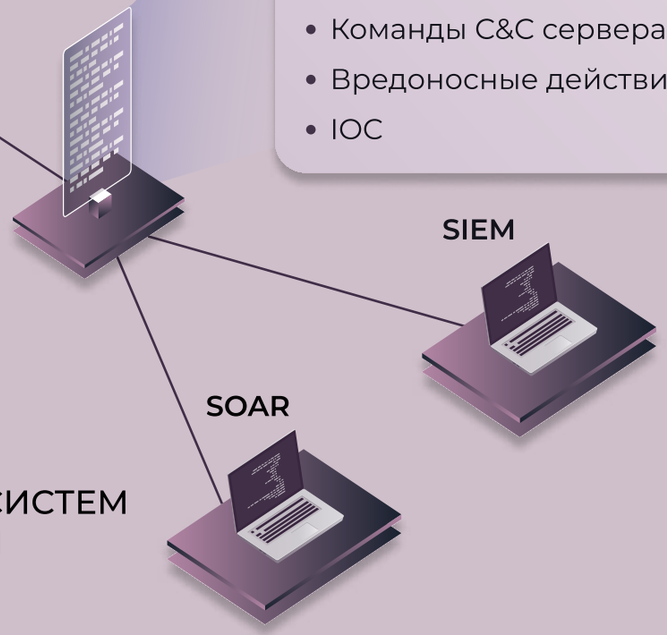
МОДУЛЬ АНАЛИЗА

Модуль анализа атаки

- Внешние аналитические источники (Suricata)
- Справочники вредоносных IP - адресов и доменов
- Анализ команд и созданных файлов

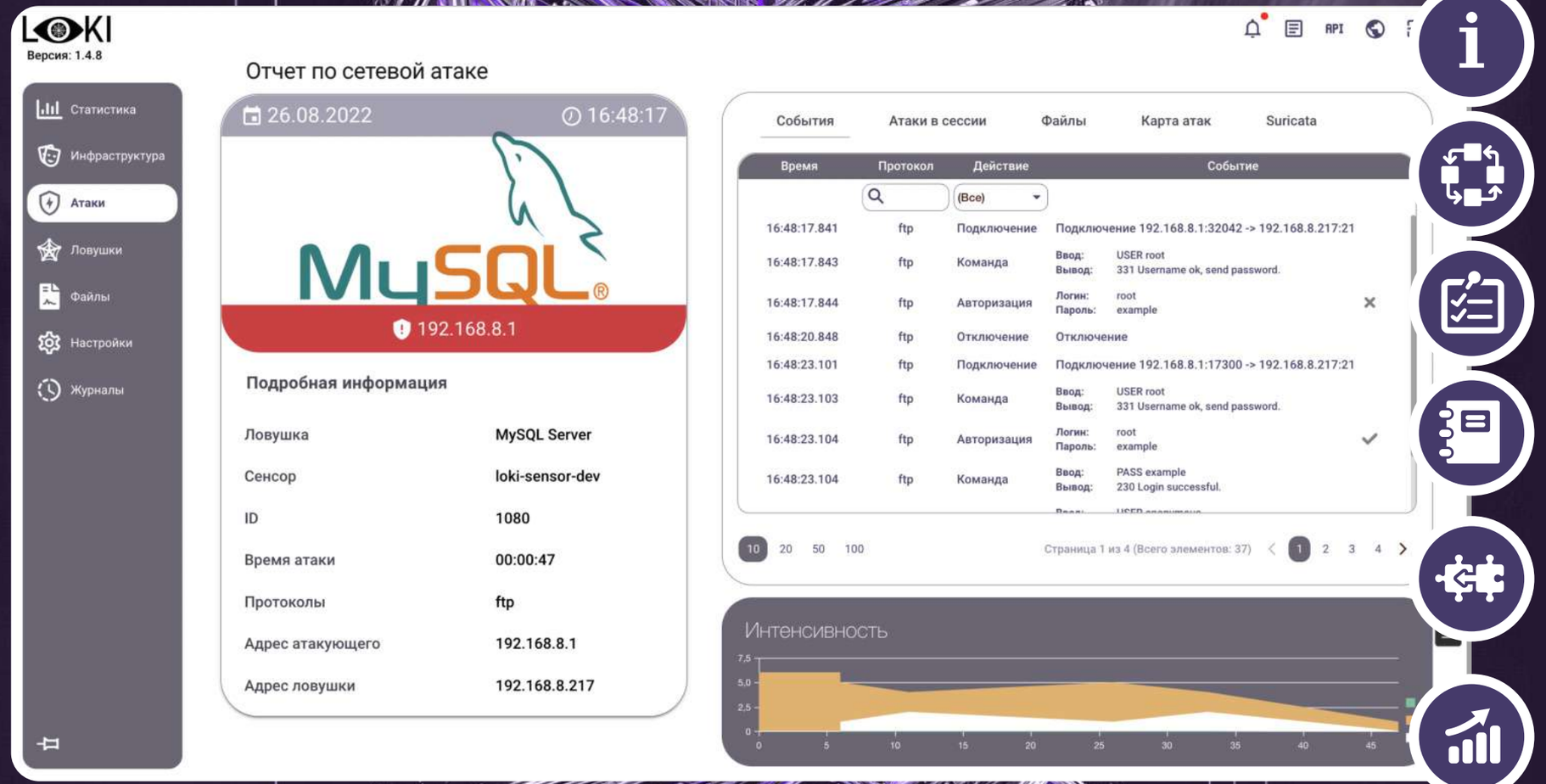
Подробный отчет

- Протоколы подключения
- Созданные файлы
- Команды C&C сервера
- Вредоносные действия
- IOC



ОПОВЕЩЕНИЕ СИСТЕМ БЕЗОПАСНОСТИ

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

СКАНИРОВАНИЕ НА УЯЗВИМОСТИ

Система LOKI осуществляет сканирование на уязвимости сервисы организации

Сканирование TCP/UPD 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

БЕЗОПАСНОСТЬ СИСТЕМЫ

Система LOKI имеет политики и настройки для обеспечения собственной безопасности

Мониторинг и обновление инфраструктурных модулей системы

Блокировка неактивных учетных записей и периодическая принудительная смена пароля

Ролевая модель с тонкой настройкой доступа к функционалу

Регистрация авторизации в системе пользователей и посредством API интерфейса

Оповещение о состоянии системы:

- обновление
- резервное копирование
- работоспособность модулей

Фиксация значимых действий всех пользователей в системе

ПРЕИМУЩЕСТВА

Мгновенная реакция на любое подключение к ловушке

Блокировка распространения угроз в рамках подсети (VLAN)

Сканирование на уязвимости реальных устройств с градацией важности

Оповещение об угрозе в системе, по электронной почте и в мессенджерах

Поддержка промышленных протоколов

Фильтрация легитимных сканирований для избежания ложных срабатываний

Отправка событий в SIEM/SOAR системы по протоколу syslog

КОНТАКТЫ

Спасибо, что нашли
время ознакомиться
с презентацией!