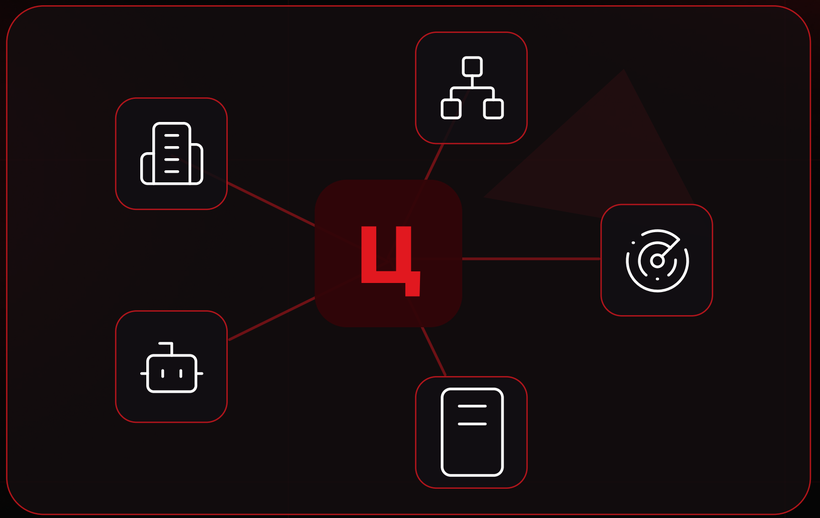
ЦМОК

управление кибербезопасностью и активами

Что такое ЦМОК?

ЦМОК — инновационная система управления безопасностью, которая позволяет организациям эффективно защищать свои сети и активы.



Для чего сделан продукт?

Платформа ЦМОК обеспечивает:

1 **Непрерывный мониторинг**

Контроль процессов информационной безопасности в режиме реального времени.

2 **Автоматизированное сканирование**

Проверка периметра компании и выявление потенциальных уязвимостей.

3 **Управление инцидентами**

Профессиональная обработка инцидентов и управление безопасностью организации.

Благодаря ЦМОК вы получаете полный контроль над безопасностью инфраструктуры, своевременно предотвращаете угрозы и минимизируете риски кибератак.

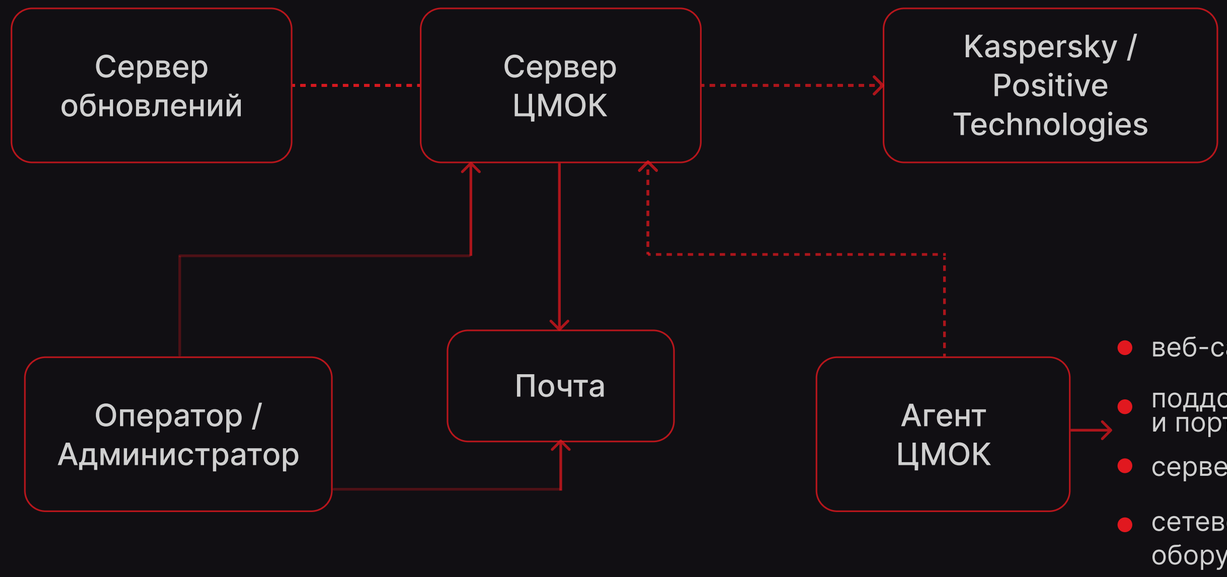
Уникальные технологии и функционал

- Интеграция с Kaspersky: KATA, KUMA, CyberTrace
- Интеграция с Positive Technologies: MaxPatrol SIEM / EDR / TI Feeds
- Интеграция с AbuseIPDB — сервисом жалоб на IP-адреса
- Высокая скорость HTTP/HTTPS запросов
- Встроенная база CVE
- Ролевая модель с разграничением доступа
- Файловое хранилище
- Экспорт отчетов в формате XLSX, PDF, CSV
- Отображение филиалов организаций на карте Республики Беларусь
- Уведомления в Telegram и на электронную почту
- Методические материалы
- Визуальное отображение топологии сети активов
- Автоматическое сканирование активов
- Статистика обнаруженных уязвимостей, портов и технологий
- Дашборд отчетности

Схема взаимодействия компонентов ЦМОК

ЦМОК состоит из двух основных компонентов — **Сервер и Агент.**

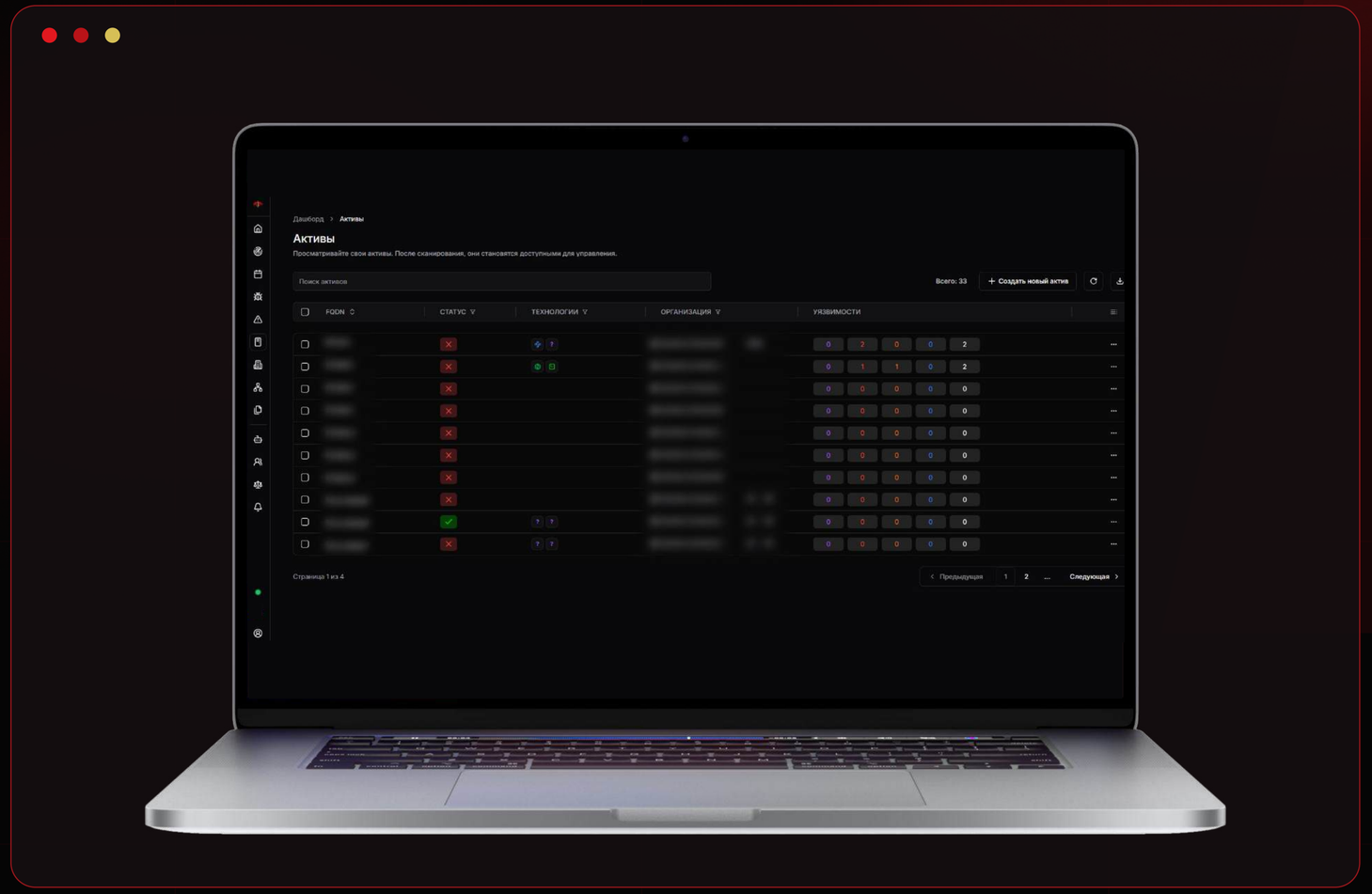
Сервер управляет агентами через веб-интерфейс. **Агенты** проводят сканирование активов организации и могут быть разделены на агенты внешнего и внутреннего периметра.



Поиск активов по IP-адресам, доменам, поддоменам

ЦМОК выявляет активы организации, обнаруживая домены, поддомены и IP-адреса.

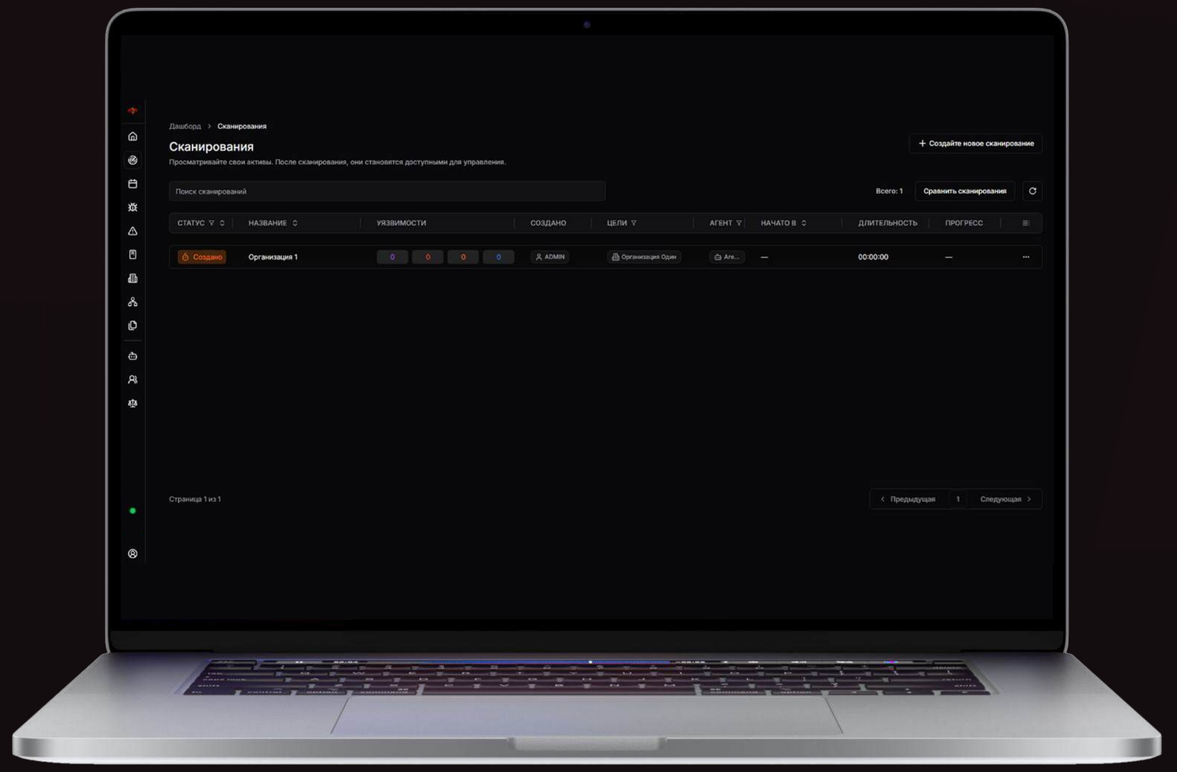
Система сбора данных позволяет обогатить эту информацию и найти максимальное количество хостов.



Анализ веб-приложений

ЦМОК выполняет глубокое сканирование веб-приложений, в том числе использующих современные технологии (SPA, PWA, реактивные фреймворки).

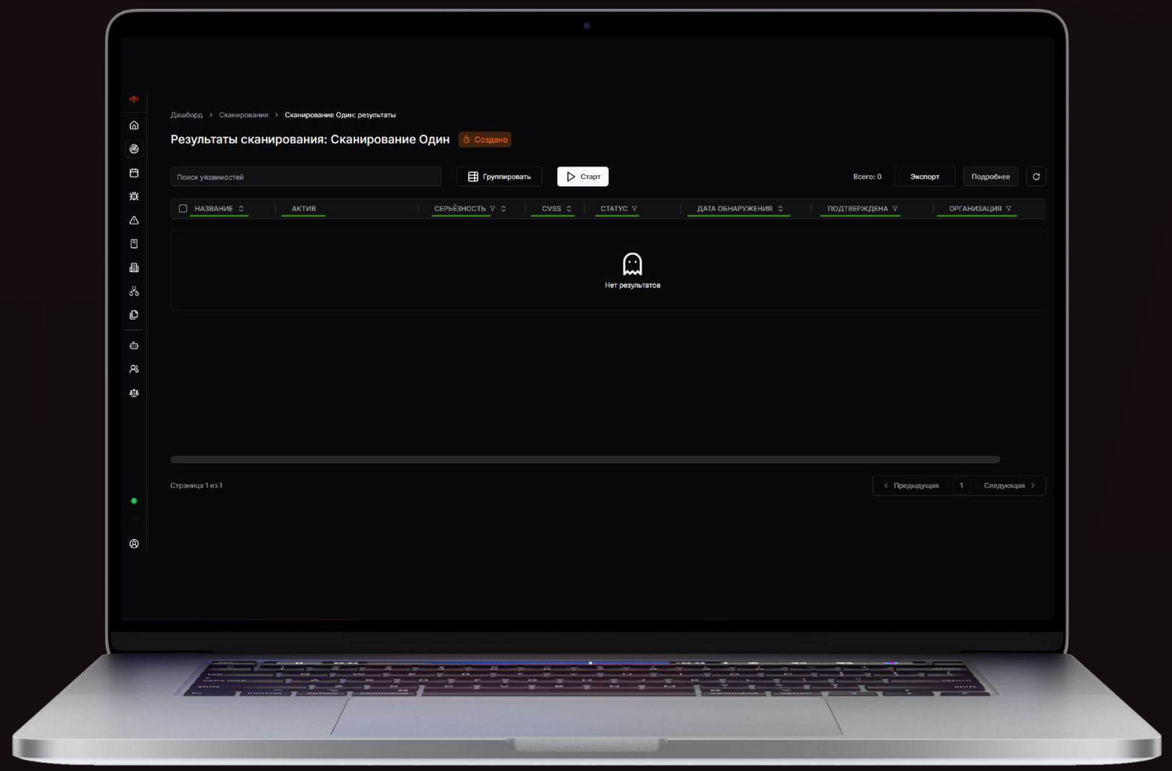
Анализ веб-приложений позволяет не только выявлять уязвимости, но и проверять формы входа на слабые или стандартные учетные данные.



Сканирование и анализ открытых портов

В процессе сканирования используется обширная база уязвимостей сервисов и служб.

ЦМОК использует несколько технологий сканирования, в том числе протоколозависимые проверки для анализа активов.



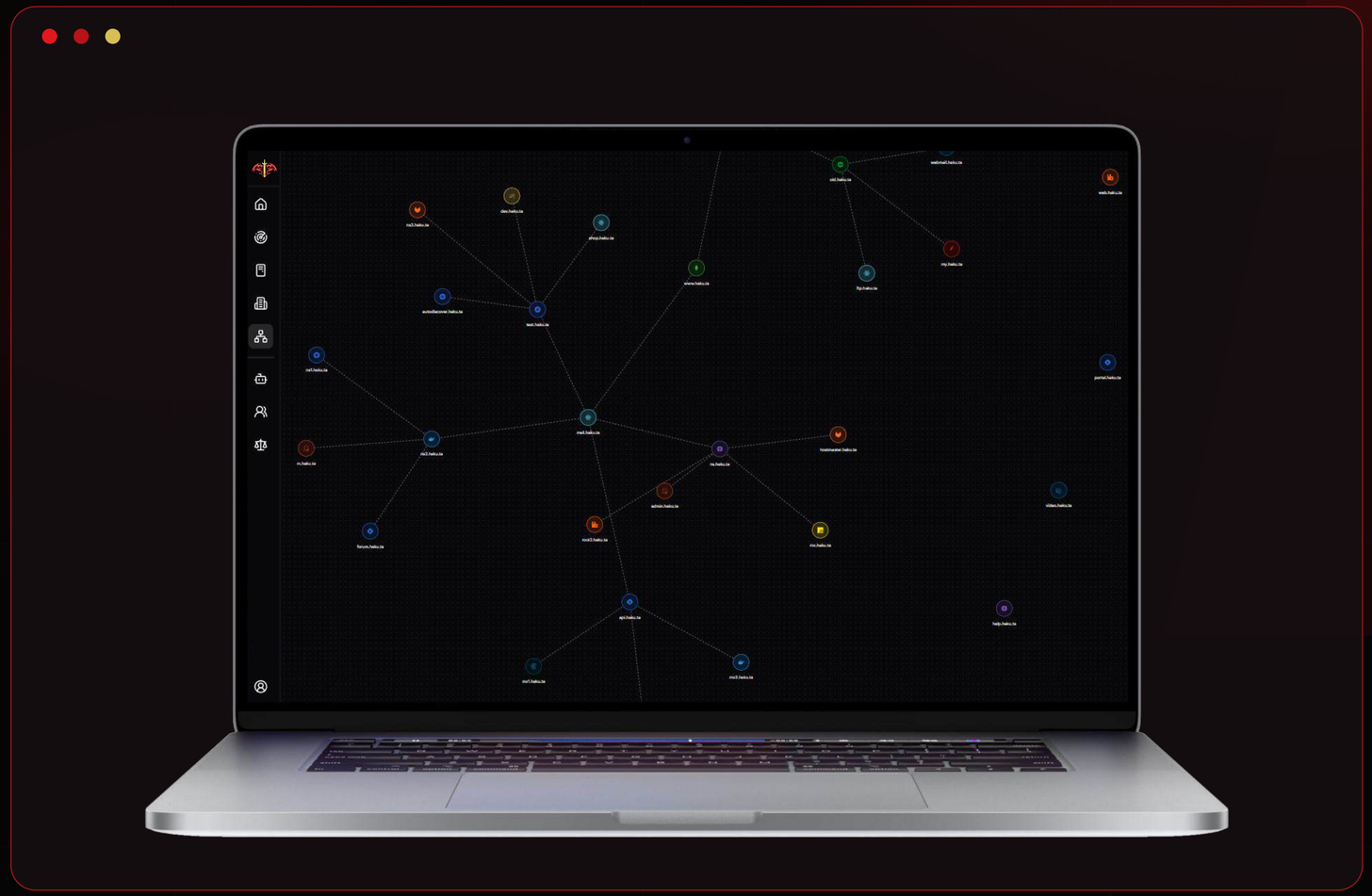
Отображение филиалов организаций на карте Республики Беларусь

ЦМОК предоставляет графическое отображение географии подключенных объектов заказчика.

Визуализация топологии сети

В процессе сканирования ЦМОК собирает информацию о сетевой топологии и строит наглядную карту сети.

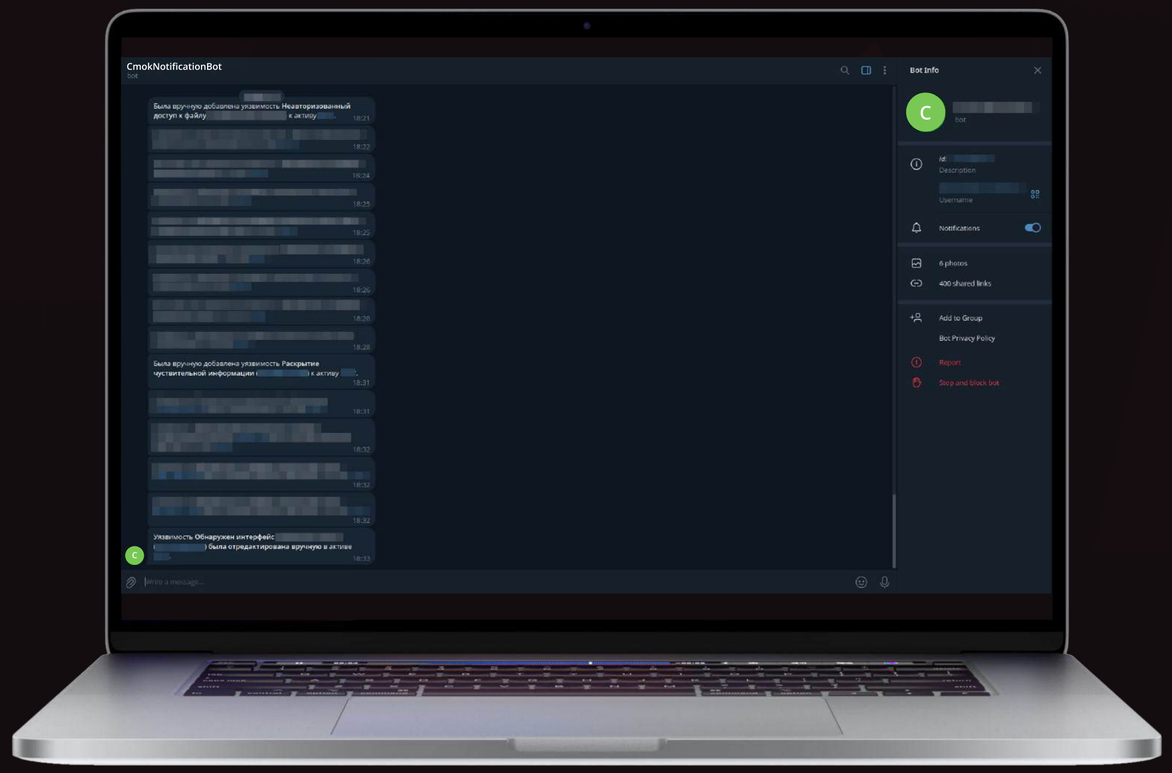
Карта сети может использоваться для обнаружения слабых мест инфраструктуры и обзора состояния информационных систем.



Отправка уведомлений в Telegram и на электронную почту

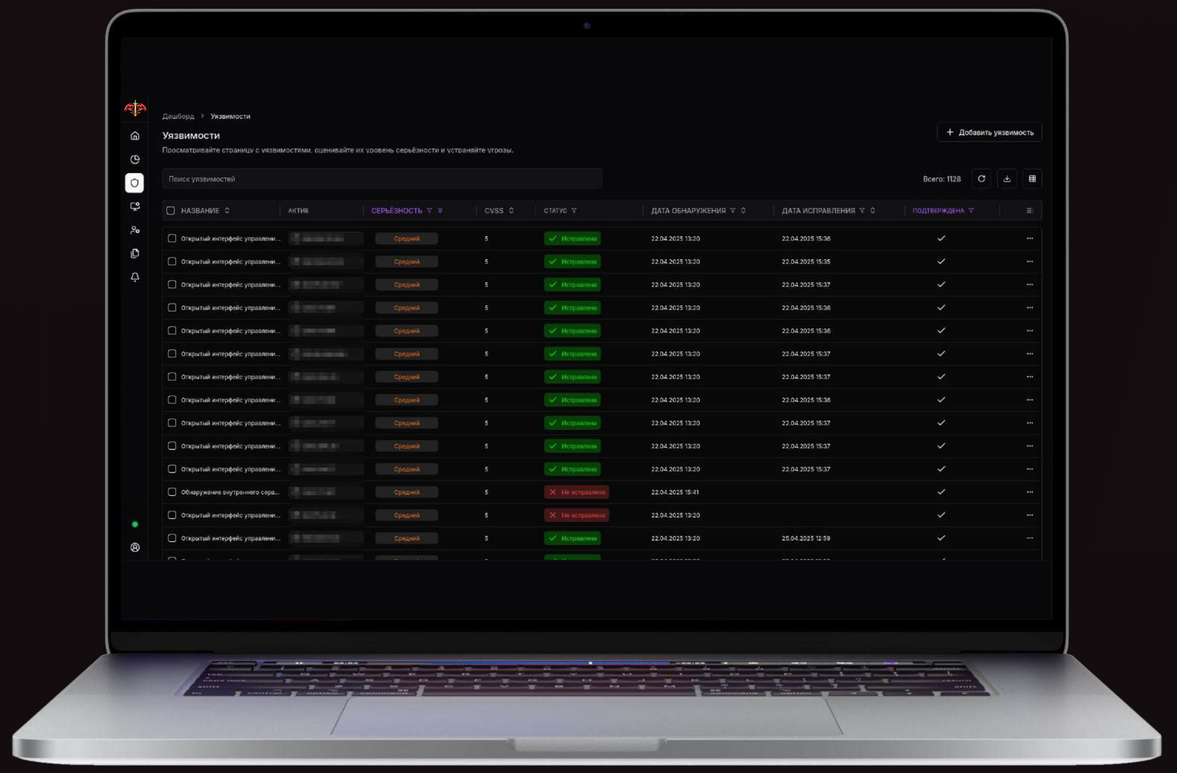
ЦМОК позволяет получать уведомления о событиях ИБ в личном кабинете, а также через мессенджер Telegram и электронную почту.

Система поддерживает гибкую настройку уведомлений, которая не даст пропустить важные сообщения и избавит уведомления от лишнего шума.



Управление уязвимостями

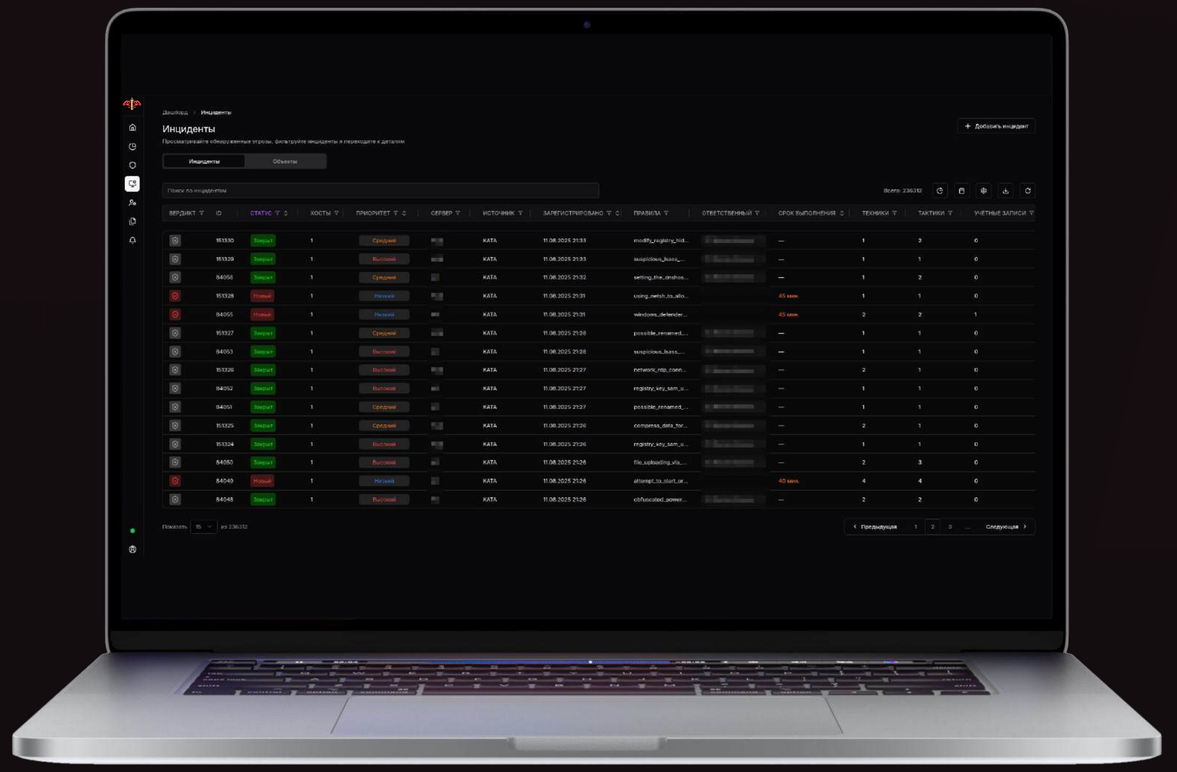
ЦМОК предоставляет комплексное решение для управления уязвимостями.
В специализированном хранилище каждая запись содержит детальное описание обнаруженной проблемы, возможные способы
её эксплуатации и связь
с соответствующим активом организации.



Управление инцидентами

ЦМОК автоматически собирает информацию о возможных угрозах с устройств, оснащенных агентом KEDR, и классифицирует их по степени критичности.

Все зафиксированные инциденты делятся на два типа: **действительные** и **ложноположительные.** Удобный дашборд наглядно отображает правила обнаружения инцидентов, что позволяет оперативно принимать решения по обеспечению безопасности.

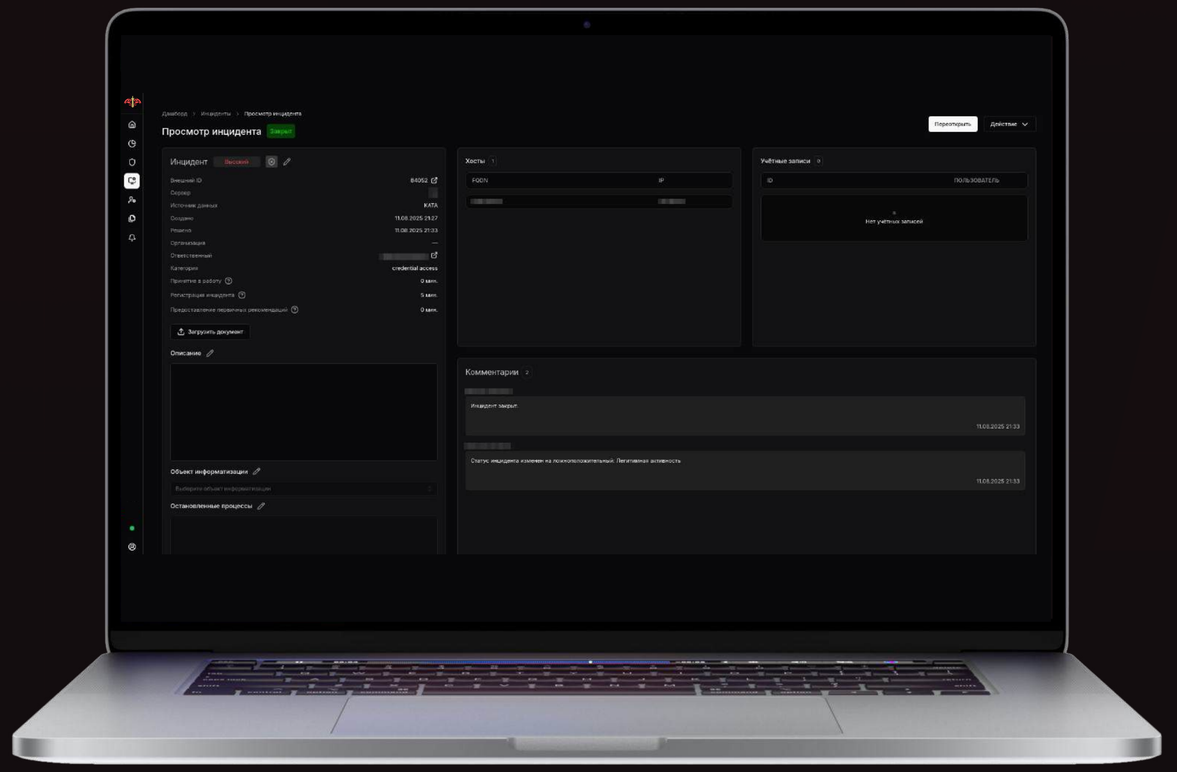


SURTE IT

Просмотр инцидента

ЦМОК позволяет отслеживать инциденты на устройствах с установленным агентом KEDR.

Подробная карточка каждого инцидента содержит время его возникновения, классификацию по матрице MITRE ATT&CK, комментарии специалистов по информационной безопасности и текущий статус, что обеспечивает быстрое реагирование на возможные угрозы.

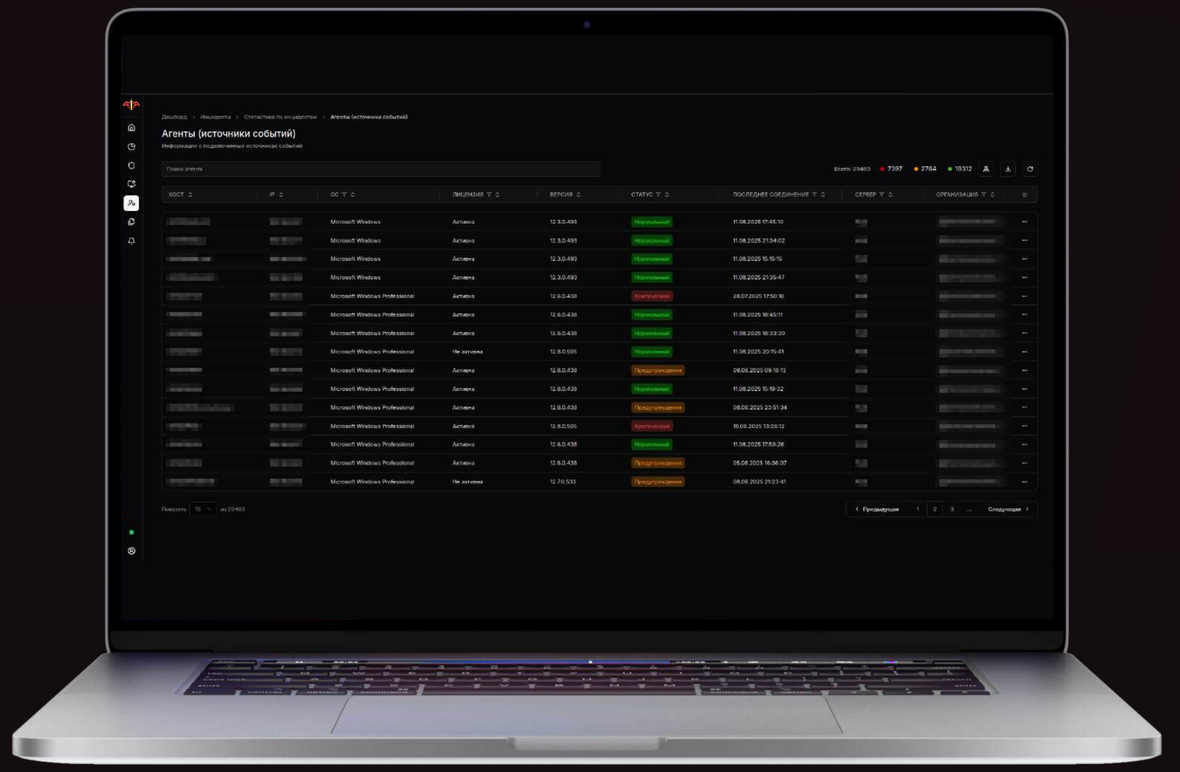


SURTE IT

Агенты KEDR

ЦМОК осуществляет сбор телеметрии с устройств, оснащенных агентами KEDR.

Благодаря этому решению вы получаете полный контроль над состоянием защищаемых устройств и можете своевременно выявлять потенциальные угрозы безопасности.



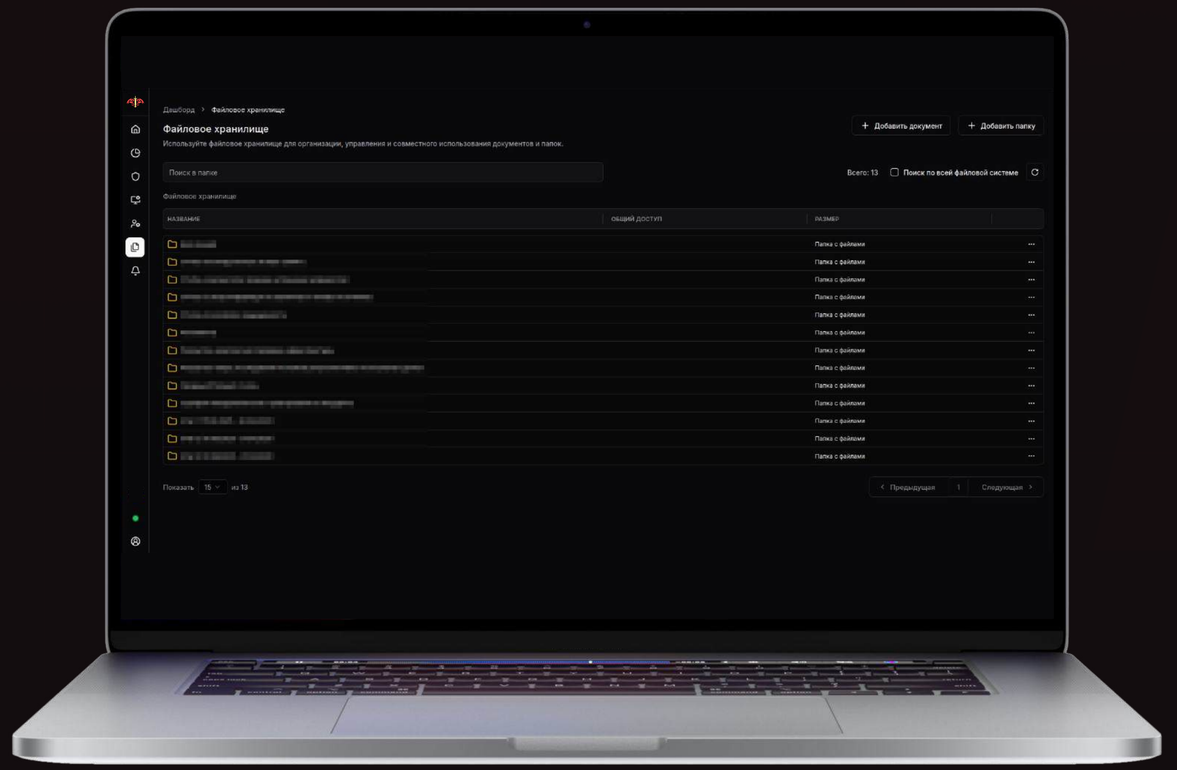
Статистика

Система формирует подробную статистику, включающую среднее количество событий в секунду (EPS) с разбивкой по организациям, отображает процент успешно закрытых инцидентов разной степени критичности и показывает актуальный статус каждого инцидента.

Управление файловым хранилищем

Система предоставляет удобный инструмент для работы с файлами — их загрузки и выгрузки.

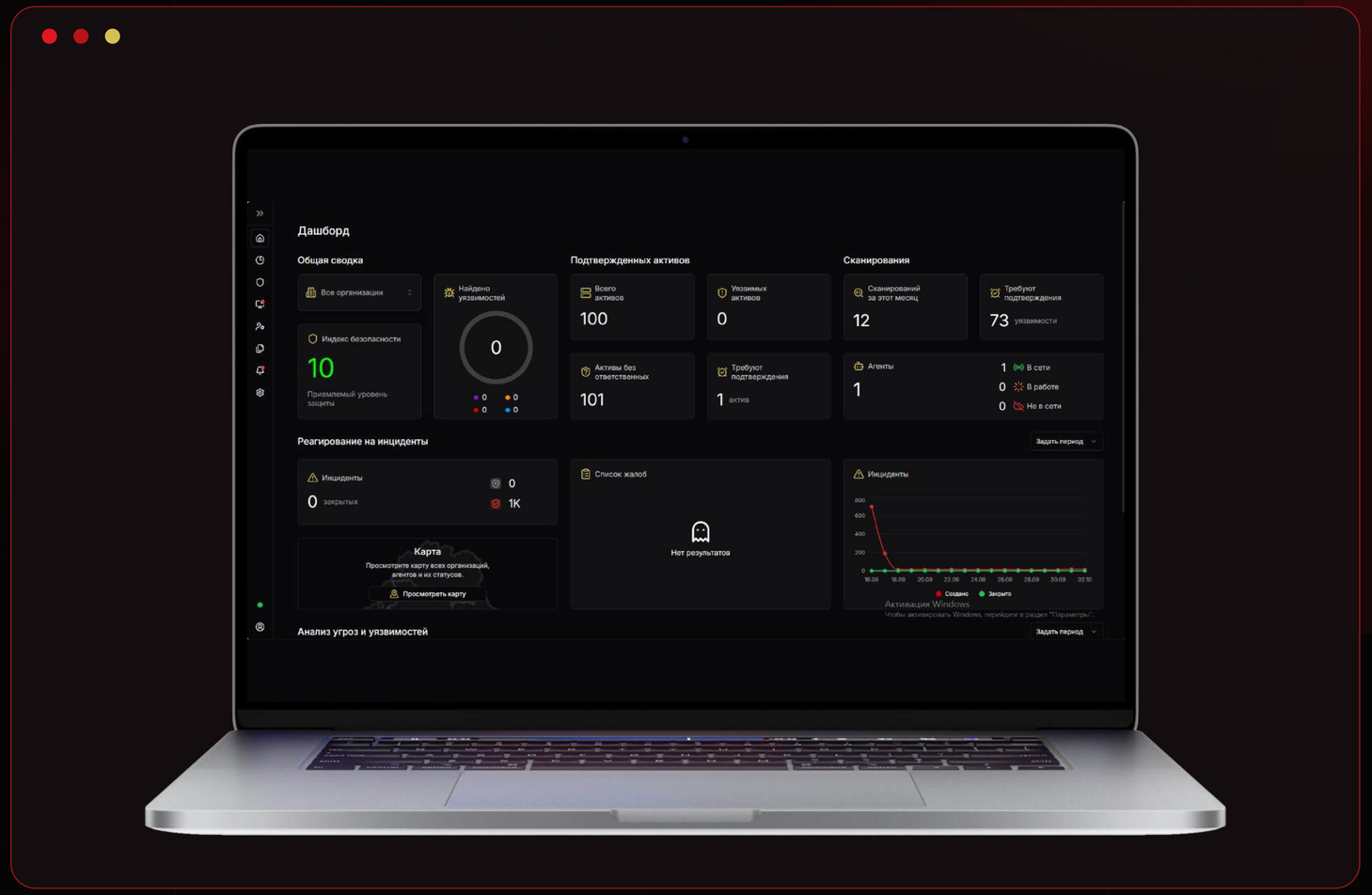
ЦМОК отличается гибкостью настроек: права доступа к файлам можно индивидуально настроить в соответствии с потребностями и требованиями организации, что обеспечивает оптимальное управление данными и их безопасность.



Дашборд

ЦМОК оснащен современным аналитическим дашбордом.

На интерактивной панели собрана подробная статистика по всем важным аспектам: информация об организациях, обнаруженных уязвимостях, установленных агентах, сетевых активах, открытых портах и общей топологии сети.



AI SOC-агент

AI SOC-агент представляет собой мультиагентную систему и использует несколько специализированных агентов для обработки инцидентов — каждый отвечает за свою область задач.

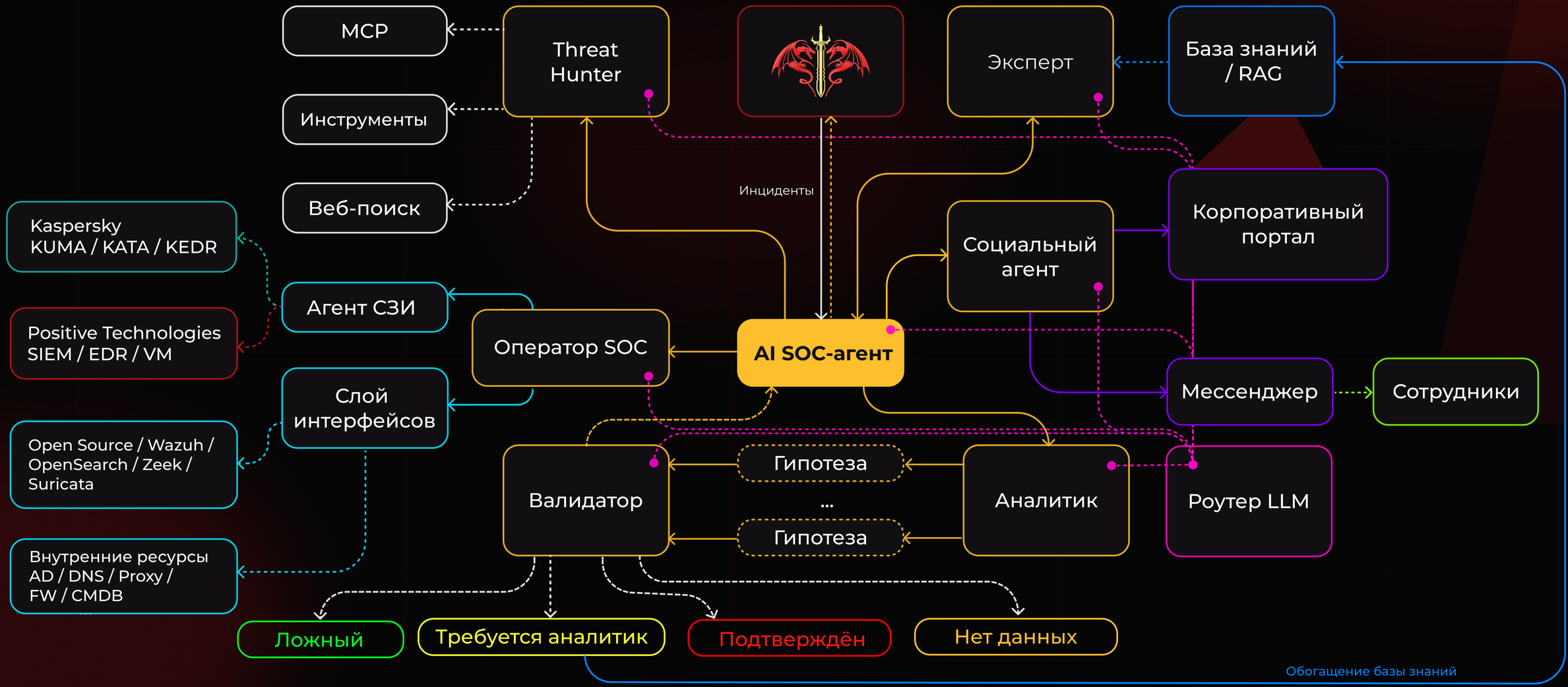
Работа не только с интегрированными СЗИ, но и с внутренними ресурсами.

AI SOC агент способен взаимодействовать с сотрудниками для обогащения информации

Система полагается не на единичные предположения, но использует множественные гипотезы — которые в ходе работы опровергаются, расширяются, или подтверждаются.

Использование и автоматическое дополнение внутренней базы знаний.

Архитектура AI SOC-агента



Трехуровневая система аналитики

L1 · первая линия аналитики

Постоянный мониторинг системы, реакция на типовые инциденты и базовая обработка событий.

L2 · вторая линия аналитики

Углубленный анализ инцидентов, изучение специфики и координация действий с L1.

L3 · третья линия аналитики

Разработка сценариев обнаружения атак, методологии и оптимизация процессов мониторинга.

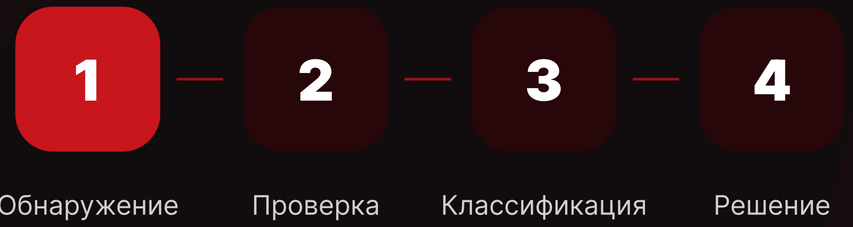
Порядок принятия решений:
Ключевые действия по изоляции систем и существенному изменению процессов принимаются строго по согласованию с руководителем подразделения и утвержденным регламентом.

Кейс №1. Процесс обработки инцидента L1-аналитиком

Первичная обработка

- Аналитик принимает инцидент в работу и проводит первичную оценку.
- Проводит проверку задействованных устройств, IP-адресов, учетных записей.

ПРОЦЕСС



Кейс №1. Процесс обработки инцидента L1-аналитиком

Анализ данных

- Переходит по ссылке в системе KATA или KUMA (ссылка доступна в карточке инцидента).
- Осуществляет проверку существующей информации в системе.

ПРОЦЕСС

Кейс №1. Процесс обработки инцидента L1-аналитиком

При легитимной активности

- Формирует комментарий с пометкой «Ложноположительный».
- Изменяет статус инцидента на «Ложноположительный».
- Инцидент переходит в статус «На проверке»

ПРОЦЕСС

Кейс №1. Процесс обработки инцидента L1-аналитиком

При вредоносной активности

- Классифицирует инцидент в соответствии с воздействием на информационную систему.
- Присваивает инциденту приоритет.
- Предпринимает первичные меры по реагированию.
- В случае необходимости эскалирует инцидент до L2-аналитика

ПРОЦЕСС

Кейс №1. Процесс обработки инцидента L2, L3-аналитиком

Углубленное расследование инцидента

- Специалист L2 производит анализ индикаторов компрометации выявленных специалистом L1.
- Собирает дополнительные индикаторы компрометации.
- Разрабатывает меры по противодействию угрозе, при необходимости производит эскалацию до L3.
- Специалист L3 производит анализ ранее неизвестной угрозы.
- Разрабатывает рекомендации и меры по противодействию угрозе.
- Разрабатывает методику реагирования на угрозы.
- Ликвидирует последствия угрозы.

ПРОЦЕСС

Кейс №1. Процесс обработки инцидента L2, L3-аналитиком

Финальное решение

Заказчик или старший смены принимает решение о переводе инцидента в статус «Закрыт» либо о направлении инцидента на доработку.

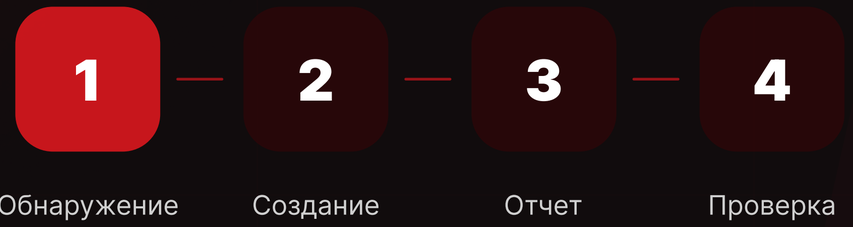
ПРОЦЕСС

Кейс №2. Процесс обработки уязвимости специалистом по ИБ

Аудит

В процессе проведения аудита безопасности специалисты обнаруживают уязвимости информационных систем.

ПРОЦЕСС



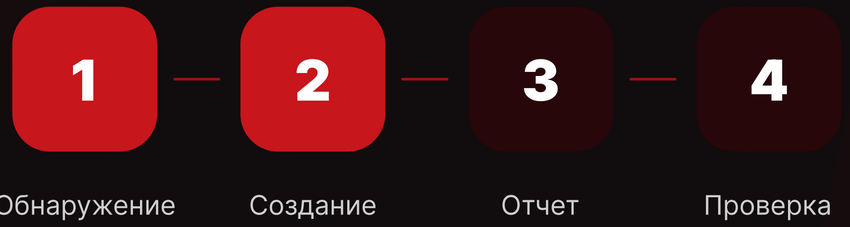
Кейс №2. Процесс обработки уязвимости специалистом по ИБ

Создание карточки уязвимости

Специалист открывает соответствующий раздел системы и выбирает опцию создания новой записи.
Специалист подробно заполняет карточку уязвимости в специальной форме:

- Название уязвимости;
- Описание;
- Критичность;
- Уязвимый актив;
- Способы эксплуатации;
- Рекомендации по устранению.

ПРОЦЕСС



Кейс №2. Процесс обработки уязвимости специалистом по ИБ

Отчет

Специалист формирует отчет в формате XLSX или CSV со списком уязвимостей за выбранный период.

ПРОЦЕСС

Кейс №3. Процесс верификации автоматически обнаруженных уязвимостей

Процедура проверки уязвимости специалистом

- Изучение подробного описания уязвимости, созданной агентом;
- Анализ дополнительных полей, заполненных агентом;
- Проведение тестовой эксплуатации;
- Проверка на наличие ложных срабатываний (false positive).

При подтверждении уязвимости специалист:

- Устанавливает соответствующий статус;
- Проводит верификацию всех данных;
- Формирует итоговый отчет;
- Передает информацию заказчику для проведения проверки и устранения проблемы.

ПРОЦЕСС

Спасибо!

Готовы показать ЦМОК в работе и обсудить внедрение с учетом особенностей вашей инфраструктуры.

surte.by vz@surte.by +375 (29) 114 81 69