KAZSIEM
Всё под контролем

Единая система мониторинга информационной безопасности организации

Иван Матвеев

Менеджер по работе с ключевыми заказчиками

+7 968 084 1488 i.matveev@kazsiem.kz

KAZSIEM

Компания, занимающаяся созданием решений в области мониторинга и управления событиями информационной безопасности и ИТ-инфраструктуры на основе анализа данных в реальном времени

Одна из ведущих высокопроизводительных и полнофункциональных SIEM-систем по соотношению цена/качество

KAZSIEM
Всё под контролем

KazSIEM сейчас

ТОП
5
SIEM-решений

10 лет
продукту
в 2024 году

x 3
рост компании за
последние 3 года

> 650
партнеров в России,
странах СНГ, Азии и
Латинской Америке

KAZSIEM
Всё под контролем

KazSIEM – это ядро системы информационной безопасности

Технология SIEM обеспечивает мониторинг и анализ событий в реальном времени, исходящих от сетевых устройств и приложений, и позволяет реагировать на них до наступления существенного ущерба

KAZSIEM
Всё под контролем

Схема работы KazSIEM

- Рабочие станции
- Firewall
- Роутеры
- Сетевые коммутаторы
- Серверы
- Мейнфреймы
- Системы обнаружения и предотвращения вторжений

SIEM

- **Предупреждения**
- **Дашборды**
- **Журнал событий**
- **Отчеты**
- **Мониторинг**

KAZSIEM
Всё под контролем

Понятный принцип работы KazSIEM

Сбор событий

Контроль инфраструктуры компании

Нормализация событий

Приведение к единому виду представления

Обогащение и симптоматика

Проверка на соответствие симптомам и добавление веса событий

Корреляция событий

Правила корреляции событий

Выявление инцидентов

Составление цепочек событий и оценка риска

KAZSIEM
Всё под контролем

Чем уникально решение KazSIEM

Не теряем события

No-code

Централизованное управление

Максимальный предустановленный функционал

Гибкость системы и компании-разработчика

Подключение любых источников данных

Разработка и поддержка от вендора

KAZSIEM
Всё под контролем

Линейка продуктов

KazSIEM
коммерческая
версия класса SIEM

KazSIEM Free
классическое решение
класса LM

KazSIEM IoC
модуль индикаторов
компрометации

KazSIEM WAF
решение для защиты
веб-приложений

KazSIEM Analytics
модуль для анализа
событий, основанный на ML

KAZSIEM
Всё под контролем

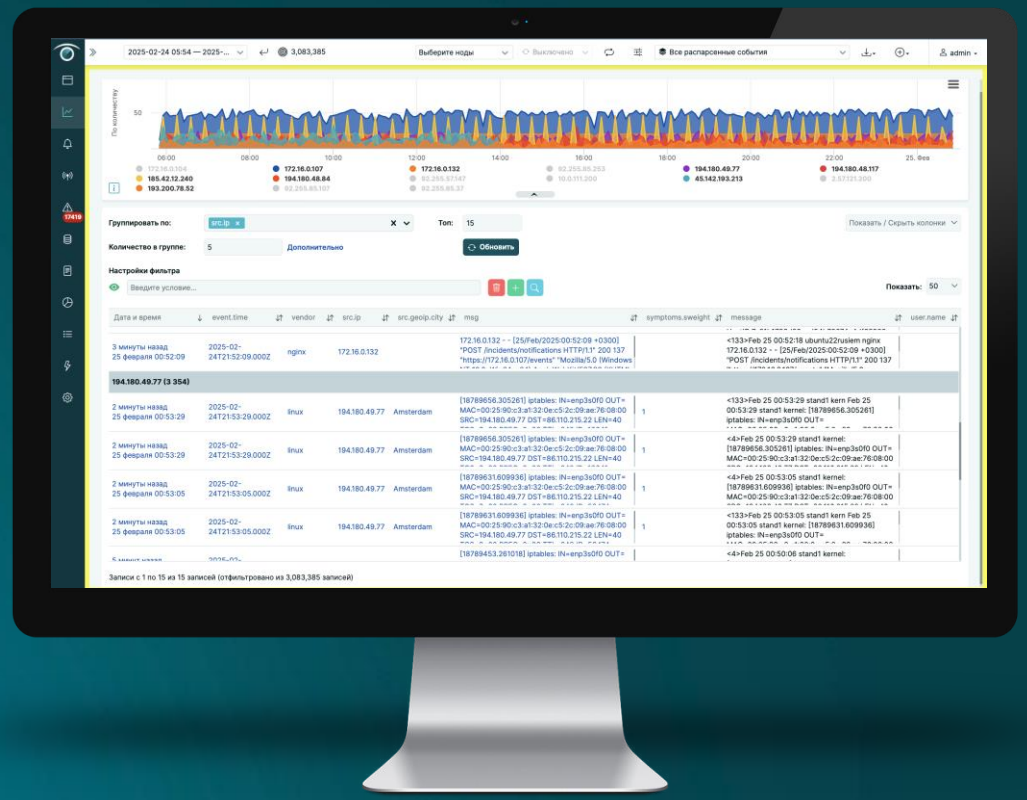
Модуль KazSIEM IoC

Позволяет выявить угрозу для корпоративных устройств в виде попыток связаться с вредоносной инфраструктурой злоумышленника

- Модуль подгружает в систему информацию об IP-адресах, доменах, URL
- Как только SIEM-система фиксирует в сетевом потоке или хостовой активности обращение к ресурсам, которые есть в базе, она сообщает об этом оператору, указывая, какой конкретно элемент ИТ-инфраструктуры скомпрометирован и требует «лечения»

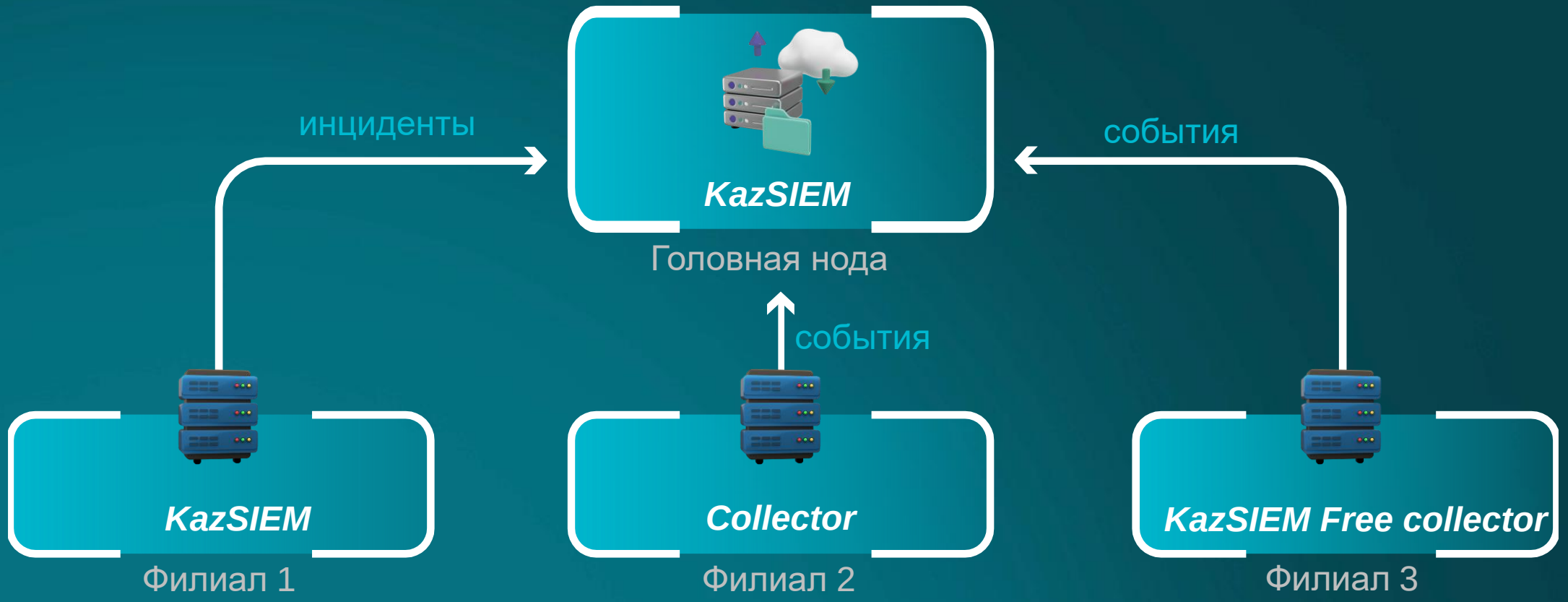
Модуль KazSIEM Analytics

- Выявление поведенческих аномалий **на основе статистики** в случаях, когда логику инцидента невозможно описать правилами корреляции
- Технологичность алгоритмов машинного обучения позволяет **выявлять на ранней стадии** и **предотвращать** возможные инциденты ИБ



KAZSIEM
Всё под контролем

Варианты развертывания системы



Лицензирование KazSIEM

- Модульные спецификации
- БЕССРОЧНЫЕ и срочные лицензии
- Разработка сложных парсеров
- Разработка правил корреляции

Количество событий в секунду

Event per second (EPS)

1 000
2 000
3 000
4 000
…

20 000
80 000
100 000
…

KAZSIEM
Всё под контролем

KazSIEM для крупного бизнеса

Безлимитная лицензия

это уникальный вид лицензирования решений KazSIEM
для действительно крупных организаций как коммерческого, так и государственного сектора

Неограниченное количество

устройств **EPS** **установок** **коллекторов**

- Гибкое управление бюджетом
- Неограниченное масштабирование под количество устройств и филиалов
- Индивидуальная поддержка и настройка под задачи бизнеса от вендора
- В среднем **на 50% выгоднее** по сравнению со стандартными лицензиями

KAZSIEM
Всё под контролем

KazSIEM WAF

Интеллектуальная система защиты веб-приложений от атак и уязвимостей для оперативного предотвращения угроз, гибкой настройки правил фильтрации и интеграции с системами ИБ

- Конструктор правил
- Гибкая система настройки правил
  - Выбор фазы работы правила
  - Возможность построения каскада правил (сработка одного правила, провоцирует работу другого)
- Малое потребление ресурсов
- Возможность запуска в контейнеризированной среде
- Высокая производительность

KAZSIEM
Всё под контролем

Лицензирование KazSIEM WAF

- Модульные спецификации
- БЕССРОЧНЫЕ лицензии
- Разработка правил

Количество запросов в секунду

Requests per second (RPS)

1
…
10 000
20 000
80 000
100 000
…

KAZSIEM
Всё под контролем

Кейс № 1

Промышленность

Портрет компании

Уже есть SIEM-система от другого вендора, но есть потребность в замене текущего решения

Особенности

Слишком дорогое обслуживание текущей инсталляции (продление системы, найм квалифицированных сотрудников, обучение). Были в поисках вариантов для миграции

Ход проекта

- Проведение демонстрации системы, обсуждение разницы в системах с точки зрения функционала, удобство пользования
- Бюджетная оценка и выдача требований к аппаратным ресурсам
- Сравнение с текущим предложением от конкурента, подготовка к пилотному проекту

KAZSIEM
Всё под контролем

Кейс № 1

Проблематика

Заказчик привык работать с другой SIEM-системой, главной сложностью было доказать удобство использования KazSIEM

Решение

Аналитиками KazSIEM было проведено обучение для заказчика, были разобраны темы написания правил нормализации и корреляции, а также подробно разобран механизм по выявлению и расследованию инцидентов

В рамках пилотного проекта была доказана возможность проведения постоянного мониторинга инфраструктуры заказчика и подведомственных организаций, которым оказывалась услуга

Итог

- **Конкурсная закупка**
- **ТЗ было написано совместно с заказчиком**

Закуплена SIEM-система от KazSIEM. Выдана лицензия, которая расширяется по мере подключения филиалов подведомственных организаций

KAZSIEM
Всё под контролем

Кейс № 2

Энергетика

Портрет компании

Выявлена потребность в SIEM-системе для закрытия требований законодательства Казахстана, организация мониторинга бизнес-процессов, приложений и инфраструктуры заказчика

Ход проекта

- Проведение демонстрации системы
- Анализ разницы в системах с точки зрения функционала, удобства использования
- Бюджетная оценка
- Выдача требований к аппаратным ресурсам

KAZSIEM
Всё под контролем

Кейс № 2

Особенности проекта

Проект был проведен без пилота на основании полученной информации в ходе демонстрации решения и выдачи бюджетной оценки

Итог

- **Конкурсная закупка**
- **ТЗ было написано вендором, по согласованию с партнером и заказчиком**

Были реализованы необходимые доработки в ходе проекта внедрения системы

KAZSIEM
Всё под контролем

Поддержка на всех этапах пилотного проекта и в процессе внедрения

Для нас главное

Слышать заказчика и понимать его потребности,
а также активно участвовать в оперативной реализации запросов

KAZSIEM
Всё под контролем

Спасибо за внимание!

Иван Матвеев

Менеджер по работе с ключевыми заказчиками

+7 968 084 1488 i.matveev@kazsiem.kz

kazsiem.kz

info@kazsiem.kz

+7 705 545 61 75

KAZSIEM
Всё под контролем