КСБ-СОФТ

SOC RAT
SECURITY OPERATION CENTER RUSSIAN ANALYTICS TEAM

МОНИТОРИНГ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (SOC)

ЗАЧЕМ ЗАЩИЩАТЬ ИНФОРМАЦИЮ

Средства защиты не успевают за стремительным развитием технологий

Информационные технологии сегодня становятся неотъемлемой частью процессов жизнеобеспечения граждан

Сторонние лица, получив доступ к конфиденциальной информации, могут нанести урон не только отдельным частным лицам или организациям, но и целому государству

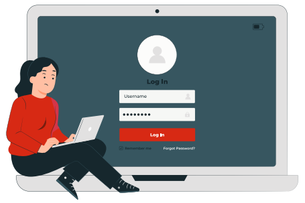
Высокий уровень компетенций злоумышленников

Злоумышленники используют многомодульный подход при осуществлении атак, умело скрывая вредоносное программное обеспечение от средств антивирусной защиты

Уязвимости и слабости конфигурации в программном обеспечении организации

Новые уязвимости появляются ежедневно, при этом на просторах Интернета легко найти готовые сценарии их эксплуатации для проведения атак

Хищение конфиденциальной информации



Нарушение доступности к ресурсам

Остановка деятельности

Потери финансов и репутации

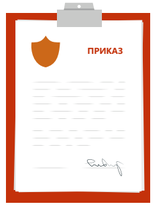
СТАНДАРТЫ И НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ

Мониторинг и реагирование на инциденты информационной безопасности – одно из требований госрегуляторов

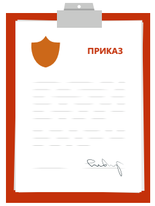
№ 149-ФЗ
о защите информации

№ 152-ФЗ
о персональных данных

№ 187-ФЗ
о безопасности КИИ



Приказ ФСТЭК № 17
о требованиях к защите информации в ГИС



Приказ ФСТЭК № 239
о требованиях к защите объектов КИИ

ГОСТ Р 59547-2021
общие положения о мониторинге информационной безопасности

Мы видим, что в 2024 году информационная безопасность как отрасль приобретает особое значение, в том числе и на государственном уровне

За 2023 год ФСТЭК России осуществил проверку свыше 350 значимых объектов КИИ. Сегодня проверки регулятора становятся все более практическими и перестают быть простым пересчетом выполненных на бумаге требований

ЧТО ТАКОЕ ЦЕНТР МОНИТОРИНГА

Схема работы Центра мониторинга

Центр мониторинга – это люди, процессы и технологии

Специалисты SOC непрерывно отслеживают сообщения, поступающие в систему мониторинга от источников: рабочих мест, серверов, средств защиты и т.д.

Из списка выявленных событий SOC-специалисты выделяют **инциденты**. Затем их задача – понять, опасен ли выявленный инцидент

Эффективность Центра мониторинга зависит от правильности выстроенных процессов, компетенций работающих в нем специалистов, а также гибкости и функциональности используемых технологий

SOC RAT

SECURITY
OPERATION
CENTER
RUSSIAN
ANALYTICS
TEAM

ЦЕНТР МОНИТОРИНГА И РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ КОМПАНИИ КСБ-СОФТ

НЕПРЕРЫВНАЯ ЗАЩИТА ОРГАНИЗАЦИЙ ОТ УГРОЗ БЕЗОПАСНОСТИ

Мониторинг 24/7

Ключевые технологии и экспертиза

Вариативность подключения

SOC по подписке

SLA в рамках рекомендаций НКЦКИ

Подключение к ГосСОПКА

КАК ЗАЩИТИТЬСЯ И ВЫПОЛНИТЬ ТРЕБОВАНИЯ РЕГУЛЯТОРОВ

Подключение к SOCRAT – это возможность

- **Выполнять** требования законодательства
- **Обеспечивать** процесс выявления событий и инцидентов
- **Выявлять** инциденты, ошибки конфигурации, уязвимости ПО, следы вредоносных программ
- **Предотвращать** инциденты, их влияние на инфраструктуру
- **Осуществлять** взаимодействие с ГосСОПКА
- **Повышать** уровень защищенности инфраструктуры

SOCRAT

Технические системы

передают аналитикам сообщения от средств защиты и компонентов информационных систем

Эксперты

отличают ложное срабатывание от «боевого»

оценивают, являются ли цепочки штатных событий началом зарождающейся атаки

прогнозируют вероятность совершения атаки

помогают клиентам отработать и расследовать инциденты

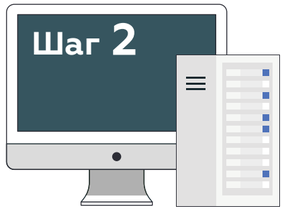
КАК SOCRAT РЕАГИРУЕТ НА ИНЦИДЕНТЫ

1 SOC-специалисты
просматривают события безопасности

Событие оказалось потенциально опасным?

НЕТ

ДА



2 SOC-специалисты
проводят первичный анализ событий безопасности

SOC-специалисты заподозрили наличие инцидента?

НЕТ

ДА

3 SOC-специалисты
создают карточку инцидента
уведомляют ответственное лицо в организации об инциденте

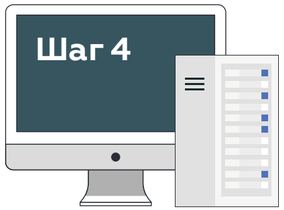
Организация подтвердила инцидент?

НЕТ

ДА

4 SOC-специалисты
делают отметку, что инцидент ложнопозитивный
закрывают инцидент

SOC-специалисты
возвращаются к просмотру событий безопасности



4 Ответственное лицо в организации
выполняет рекомендации Центра мониторинга

SOC-специалисты
закрывают инцидент
усиливают контроль за угрозами безопасности

SOC-специалисты
возвращаются к просмотру событий безопасности

Слушайте наш подкаст о том, как SOCRAT противодействует современным угрозам и защищает контролируемые организации

ПАКЕТЫ ПОДКЛЮЧЕНИЯ К SOCRAT

БАЗОВЫЙ ПАКЕТ «КОНТРОЛЬ»

Мониторинг и реагирование
на инциденты ИБ

ПАКЕТ «ПРЕДУПРЕЖДЕНИЕ»

Инвентаризация

Анализ уязвимостей

Тестирование на проникновение

ПАКЕТ «РАССЛЕДОВАНИЕ»

Глубокая аналитика

Расследование инцидентов
и поиск причин их появления

ГОССОПКА

ПАКЕТ «ГосСОПКА»

Разработка рабочей документации

Передача информации
об инцидентах в ГосСОПКА

Получение от НКЦКИ рекомендаций
и направление их в контролируемую
организацию

Рекомендованные схемы подключения

РОИВ/ФОИВ

БАЗОВЫЙ ПАКЕТ «КОНТРОЛЬ»

ПАКЕТ «ПРЕДУПРЕЖДЕНИЕ»

Субъекты КИИ

БАЗОВЫЙ ПАКЕТ «КОНТРОЛЬ»

ПАКЕТ «ПРЕДУПРЕЖДЕНИЕ»

ПАКЕТ «ГосСОПКА»

Коммерческие организации

БАЗОВЫЙ ПАКЕТ «КОНТРОЛЬ»

ПАКЕТ «ПРЕДУПРЕЖДЕНИЕ»

ПАКЕТ «РАССЛЕДОВАНИЕ»

ПИЛОТНОЕ ПОДКЛЮЧЕНИЕ

Вы можете бесплатно оценить качество предоставляемых услуг SOCRAT

Что входит в пилотное подключение?

мониторинг в режиме 8 x 5

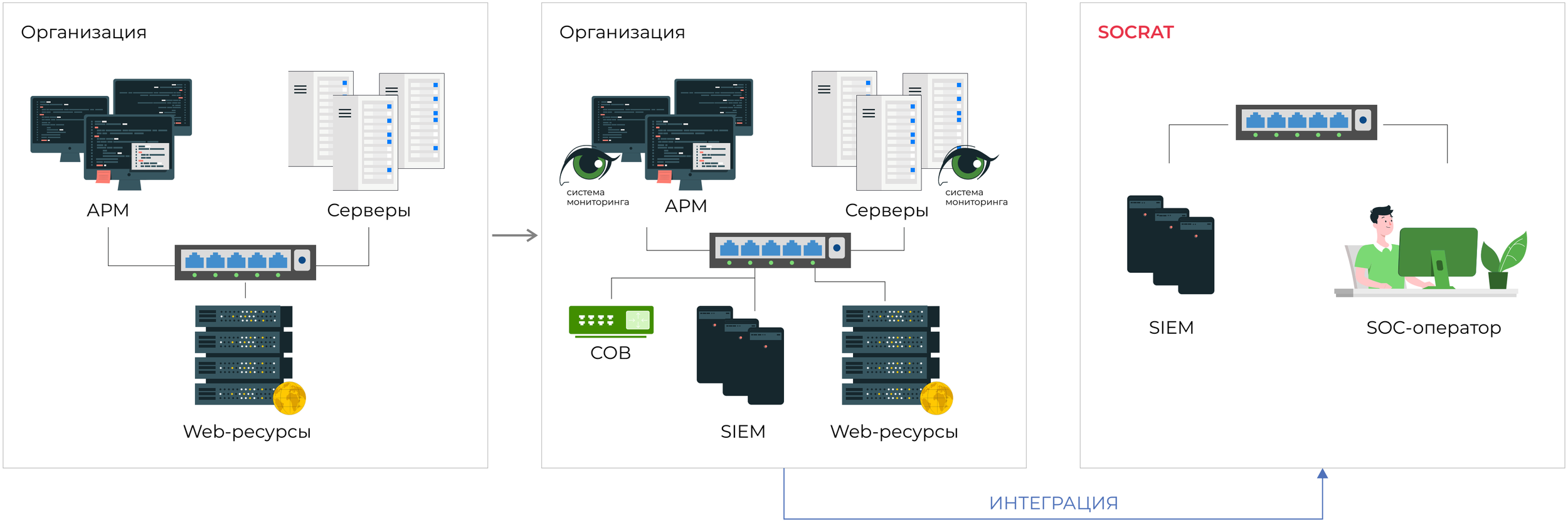
время реакции на инцидент – до 24 часов с момента обнаружения (без учета выходных и праздничных дней)

состав контролируемых узлов – до 10 узлов (АРМ/серверы) и/или 1 система обнаружения вторжений уровня сети

длительность пилота – один календарный месяц

ВАРИАНТЫ ПОДКЛЮЧЕНИЯ К ЦЕНТРУ МОНИТОРИНГА SOCRAT

Вариант 1. Построение системы мониторинга с нуля



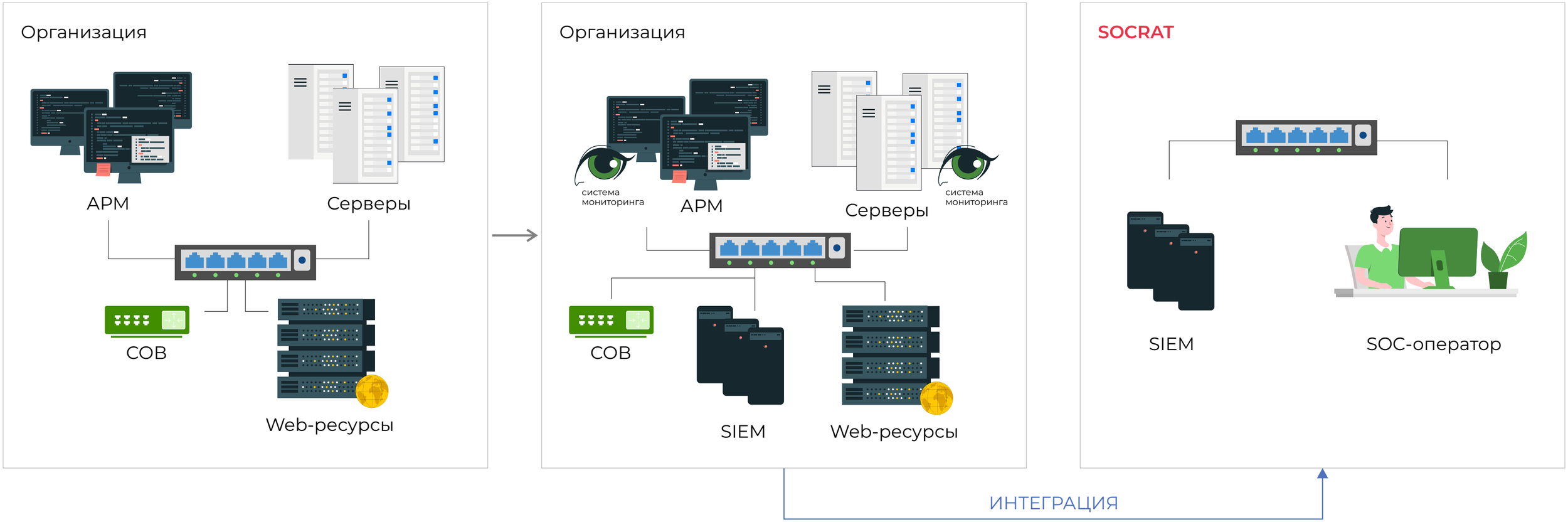
Команда SOCRAT проводит работы с помощью системы мониторинга

Поэтому при отсутствии такой системы в организации мы поможем спроектировать её, приобрести и внедрить все необходимые компоненты, а также настроить их работу

А затем мы проведем интеграцию построенной системы мониторинга с системой SOCRAT

ВАРИАНТЫ ПОДКЛЮЧЕНИЯ К ЦЕНТРУ МОНИТОРИНГА SOCRAT

Вариант 2. Развитие существующей системы мониторинга

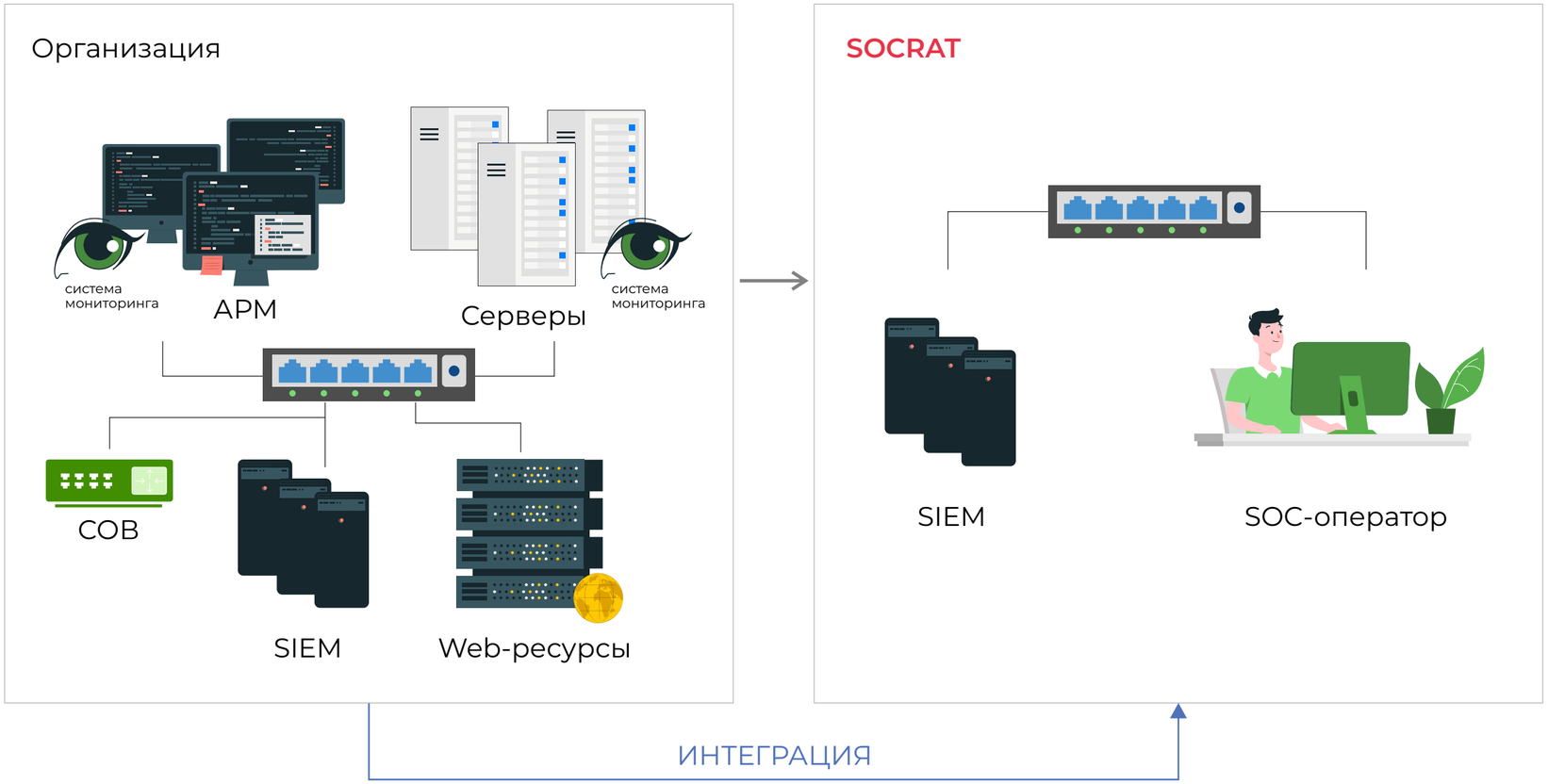


Если вы уже закупили отдельные устройства для системы мониторинга, мы поможем подобрать и внедрить недостающие компоненты, а также настроить их работу

А затем мы проведем интеграцию доработанной системы мониторинга с системой SOCRAT

ВАРИАНТЫ ПОДКЛЮЧЕНИЯ К ЦЕНТРУ МОНИТОРИНГА SOCRAT

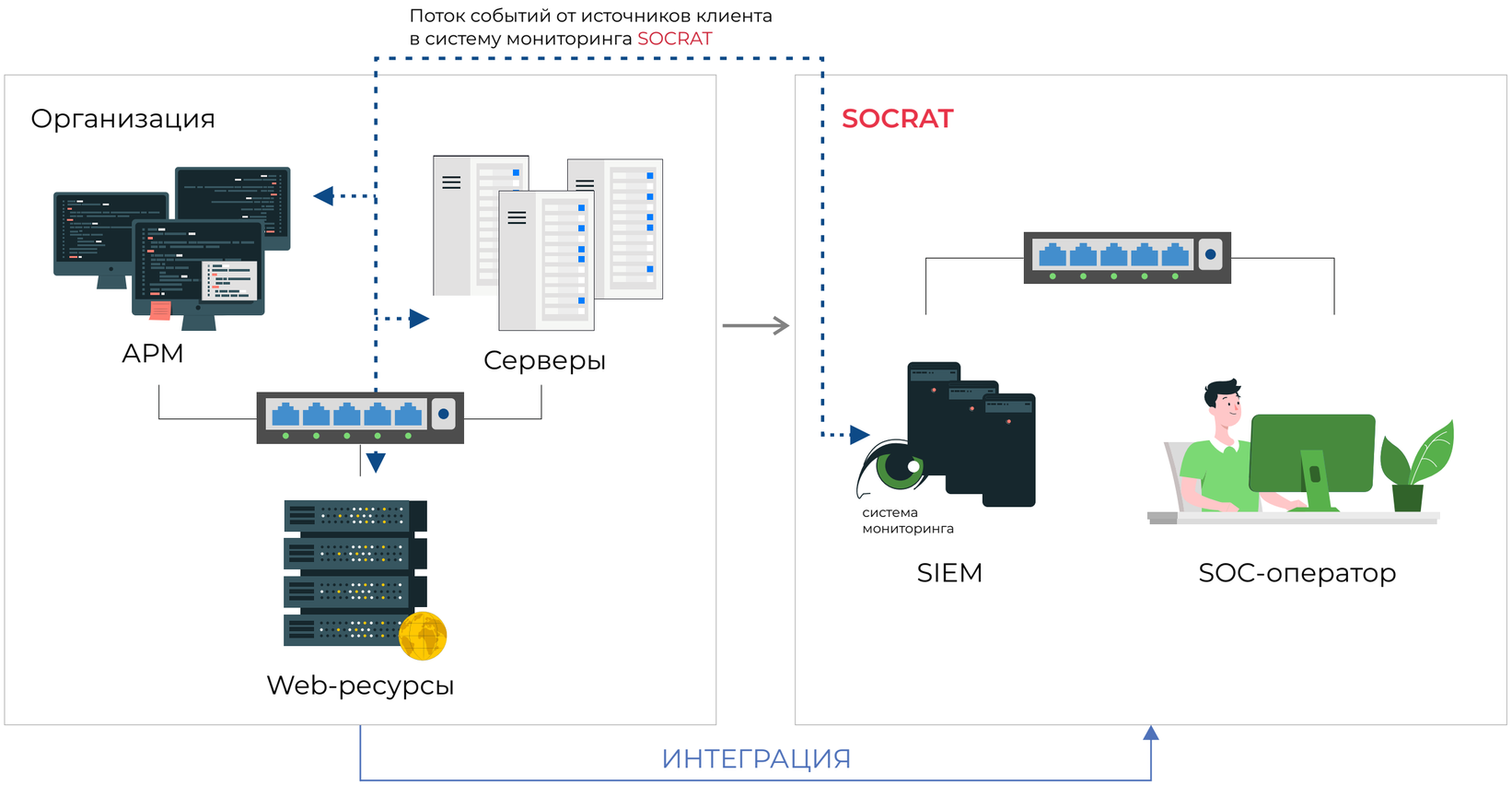
Вариант 3. Интеграция имеющейся в организации системы мониторинга с системой SOCRAT



Если вы уже построили собственную систему мониторинга, но в штате организации отсутствуют SOC-специалисты, которые могут контролировать безопасность инфраструктуры, мы проведем интеграцию вашей системы с системой SOCRAT

ВАРИАНТЫ ПОДКЛЮЧЕНИЯ К ЦЕНТРУ МОНИТОРИНГА SOCRAT

Вариант 4. SOC по подписке



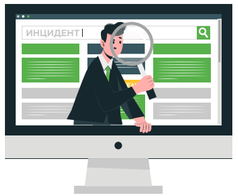
Если у вас нет возможности построить систему мониторинга в своей инфраструктуре, а также нет специалистов для организации непрерывного процесса мониторинга и реагирования на инциденты безопасности, мы предлагаем облегченный вариант подключения

Наша команда при помощи агентов либо безагентным способом подключит ваши источники событий к системе мониторинга SOCRAT и организует процесс непрерывного мониторинга специалистами нашего центра

ЧТО В ИТОГЕ?

Выявление всех подозрительных событий безопасности и дальнейшая их отработка

Своевременное реагирование и противодействие инцидентам информационной безопасности



Расследование инцидентов безопасности и помощь в устранении их последствий

Соответствие законодательным требованиям

ПОЧЕМУ ИМЕННО МЫ?

SOCRAT – это ваша возможность получить:

Мониторинг 24/7
круглосуточный мониторинг инцидентов безопасности аналитиками SOC

Ключевые технологии и экспертиза SOCRAT
синергетический эффект применения передовых технологий и накопленного опыта экспертов SOCRAT

Вариативность подключения
выбор варианта подключения исходя из потребностей, особенностей инфраструктуры и финансовых возможностей организации

SOC по подписке
подключение к SOC по MSSP-модели за 3 дня*

SLA в рамках рекомендаций НКЦКИ
базовый режим – 24 часа
расширенный режим – 3 часа**

Подключение к ГосСОПКА
организация взаимодействия с НКЦКИ

* - зависит от срока поставки лицензии вендором/дистрибьютером и может быть увеличено до 14 дней
** - более сжатые сроки реагирования обсуждаются индивидуально

КОМПАНИЯ КСБ-СОФТ

Системный интегратор в сфере информационной безопасности и импортозамещения информационных технологий

Мониторинг и реагирование на инциденты ИБ

Аудит информационной безопасности

Анализ уязвимостей и тестирование на проникновение

Обеспечение безопасности КИИ и АСУ ТП

Внедрение процессов безопасной разработки

Защита информации в ГИС и ИСПДн

Наш вклад в кибербезопасность

Защита значимых объектов КИИ РФ

Разработанные командой КСБ-СОФТ специализированные утилиты и скрипты для тестирования безопасности ИТ-инфраструктуры организаций

Активная деятельность в российском сообществе по безопасной разработке

Наши клиенты – государственные и коммерческие организации в 80 регионах России

На сегодня в портфолио компании более 4000 проектов разной степени сложности, полученный опыт в которых помогает нам подбирать эффективные решения для защиты информационных ресурсов наших клиентов

SOC RAT

SECURITY
OPERATION
CENTER
RUSSIAN
ANALYTICS
TEAM

SOCRAT – ЦЕНТР ПРОТИВОДЕЙСТВИЯ КИБЕРАТАКАМ

КСБ-СОФТ

8 800 3333-872

+7 (8352) 322-322

info@ksb-soft.ru

КАНАЛ
«МНЕНИЕ ИНТЕГРАТОРА»

ПОДКАСТ
«SOCRAT ЗА СТЕКЛОМ»

САЙТ
КОМПАНИИ