КСБ-СОФТ

SOC RAT
SECURITY OPERATION CENTER RUSSIAN ANALYTICS TEAM

МОНИТОРИНГ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (SOC)

ЗАЧЕМ ЗАЩИЩАТЬ ИНФОРМАЦИЮ

Стремительное развитие 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, когда некоторые ее этапы могут проводиться разными группировками

Кроме того, злоумышленники научились умело скрывать 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

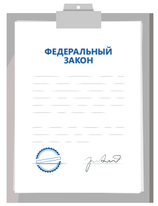
Остановка деятельности

Потери финансов и репутации

СТАНДАРТЫ И НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ

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

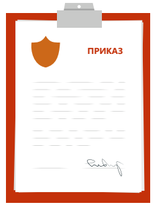
№ 149-ФЗ
о защите информации



№ 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

Сегодня мы видим, что информационная безопасность как отрасль приобретает особое значение, в том числе и на государственном уровне

Осенью прошлого года заместитель председателя правительства Дмитрий Чернышенко в докладе Президенту определил ее особую роль, заявив, что число кибератак на российскую инфраструктуру в 2022 году увеличилось на 80% по сравнению с предыдущим периодом

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 инцидентов ИБ в режиме 24/7

Вариативность при подключении

Высокий SLA – моментальное реагирование на инциденты

Индивидуальный подход к потребностям компании
и особенностям ее инфраструктуры

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

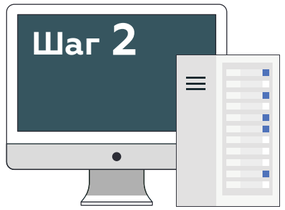
КАК SOCRAT РЕАГИРУЕТ НА ИНЦИДЕНТЫ

1 SOC-специалисты
просматривают события безопасности

НЕТ

Событие оказалось потенциально опасным?

ДА



2 SOC-специалисты
проводят первичный анализ событий безопасности

НЕТ

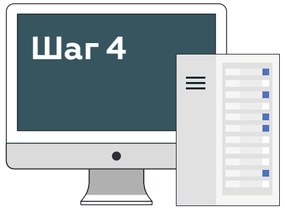
SOC-специалисты заподозрили наличие инцидента?

ДА

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

Организация подтвердила инцидент?

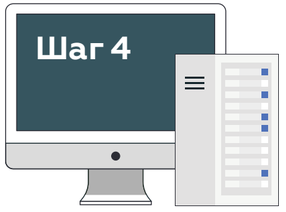
НЕТ



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

SOC-специалисты
возвращаются к просмотру событий безопасности

ДА



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

Сканируйте qr-код и читайте живую историю о том, как работает SOC

SOCRAT ПРЕДЛАГАЕТ

Полный комплекс услуг по мониторингу и реагированию на инциденты информационной безопасности

БАЗОВЫЙ ПАКЕТ «КОНТРОЛЬ»

Мониторинг и реагирование на инциденты ИБ

ДОП. ПАКЕТ «ПРЕДУПРЕЖДЕНИЕ»

Инвентаризация
Анализ уязвимостей
Тестирование на проникновение

ДОП. ПАКЕТ «ПРОТИВОДЕЙСТВИЕ»

Глубокое расследование инцидентов
Взаимодействие с ГосСОПКА

ПИЛОТНОЕ ПОДКЛЮЧЕНИЕ

Вы можете бесплатно оценить качество предоставляемых услуг SOCRAT

Что входит в пилотное подключение?

мониторинг в режиме 8x5 (8:00 до 17:00 по МСК)

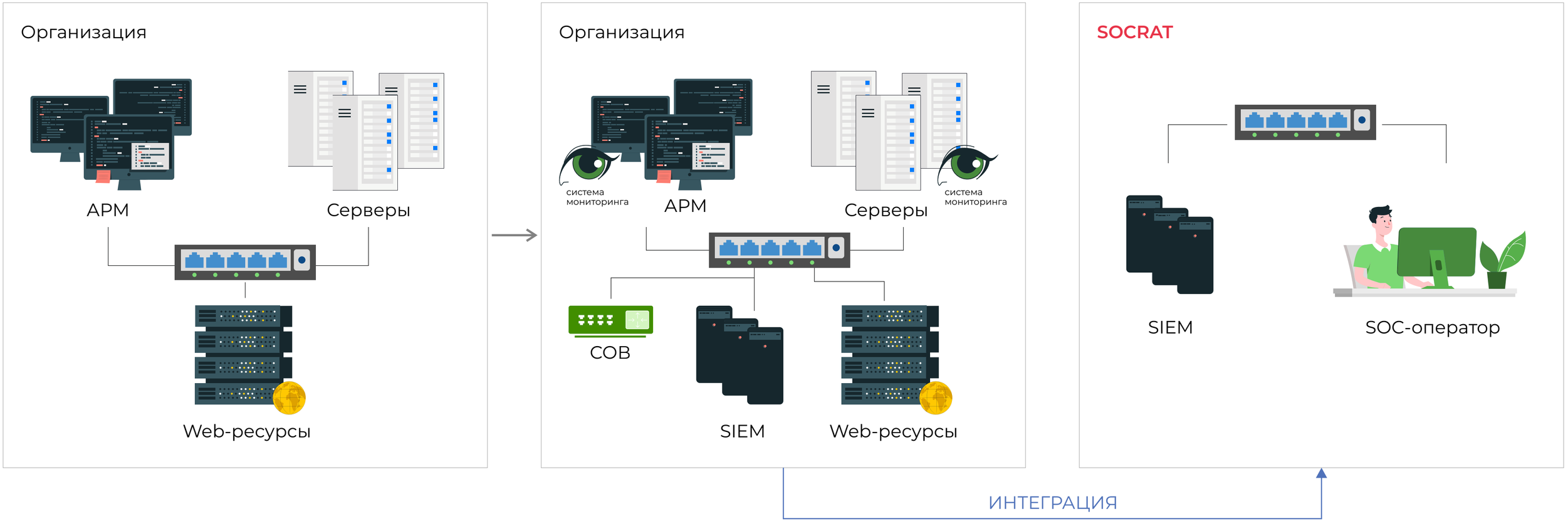
время реакции на инцидент – до 24 часов с момента обнаружения (без учета выходных и праздничных дней)

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



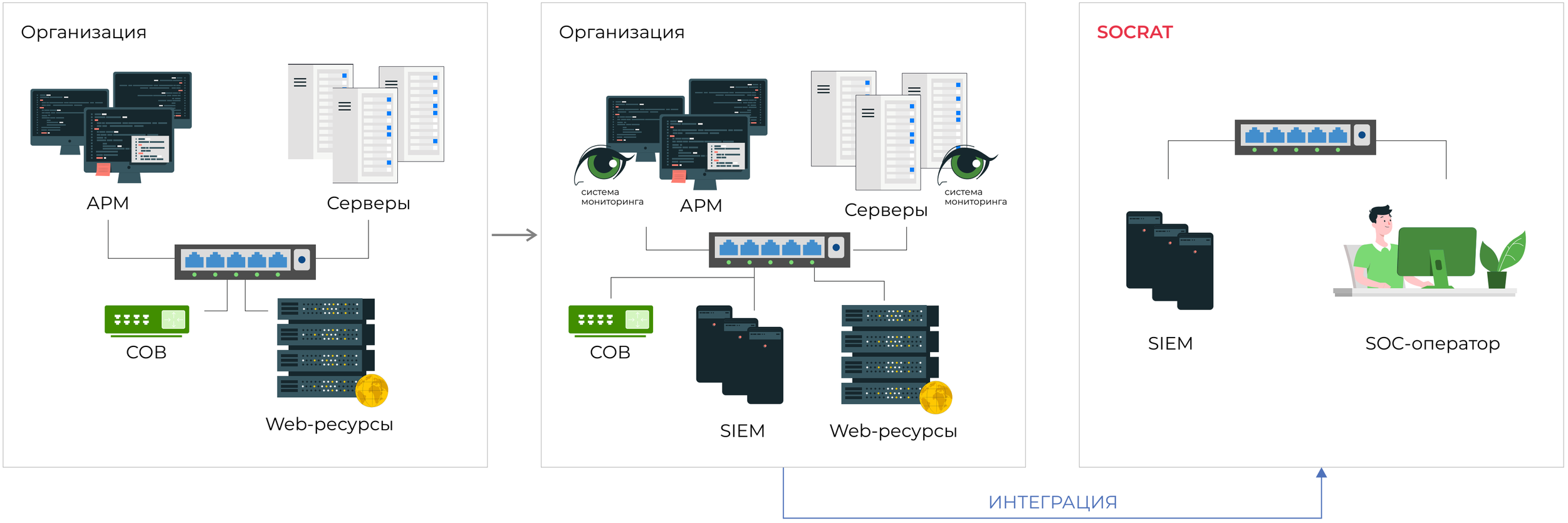
Команда SOCRAT проводит работы с помощью системы мониторинга

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

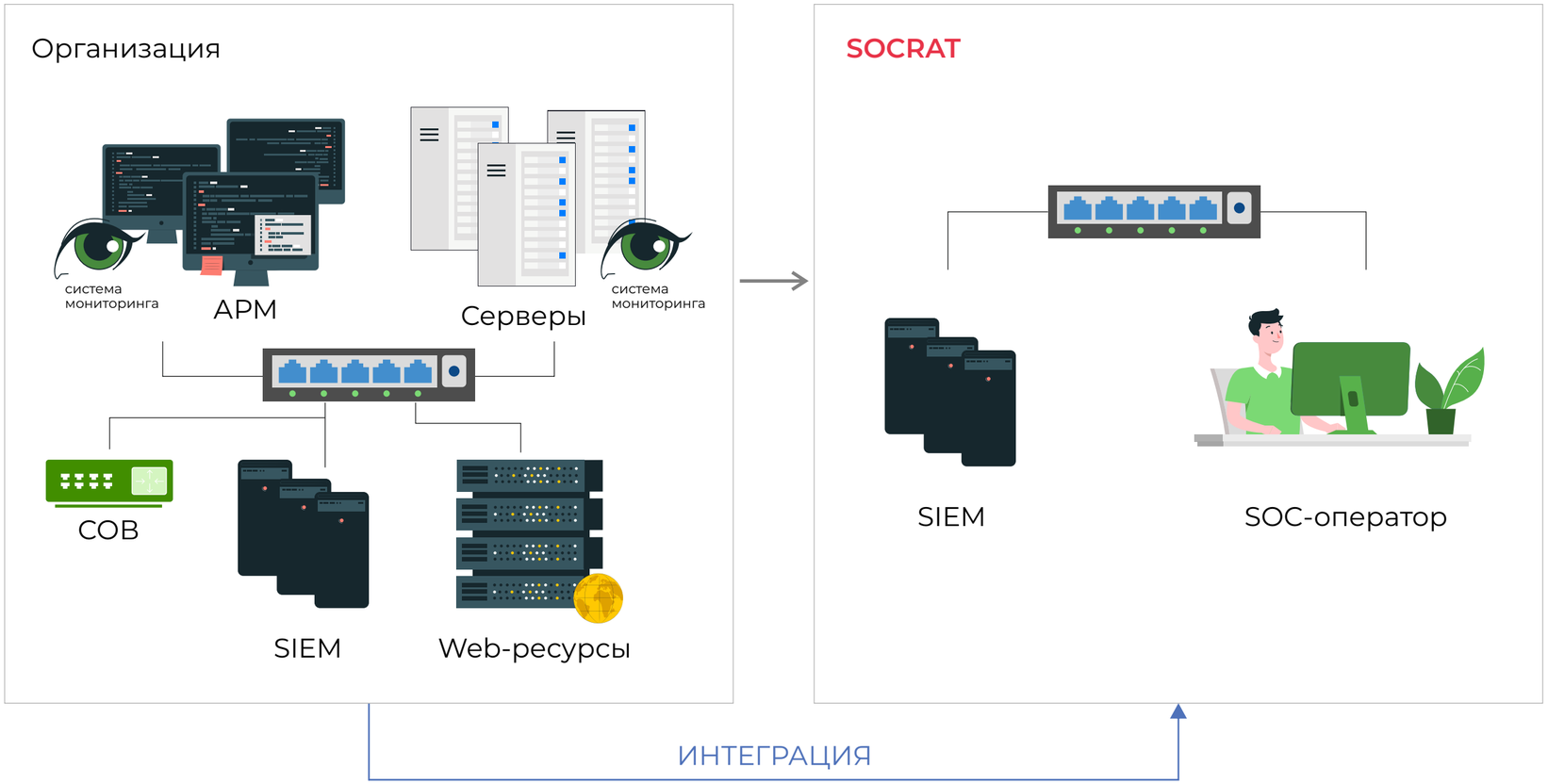


Если вы уже закупили отдельные устройства для системы мониторинга, мы поможем подобрать и внедрить недостающие компоненты, а также настроить их работу

А затем мы проведем интеграцию доработанной системы мониторинга с системой SOCRAT

ВАРИАНТЫ ПОДКЛЮЧЕНИЯ К ЦЕНТРУ МОНИТОРИНГА SOCRAT

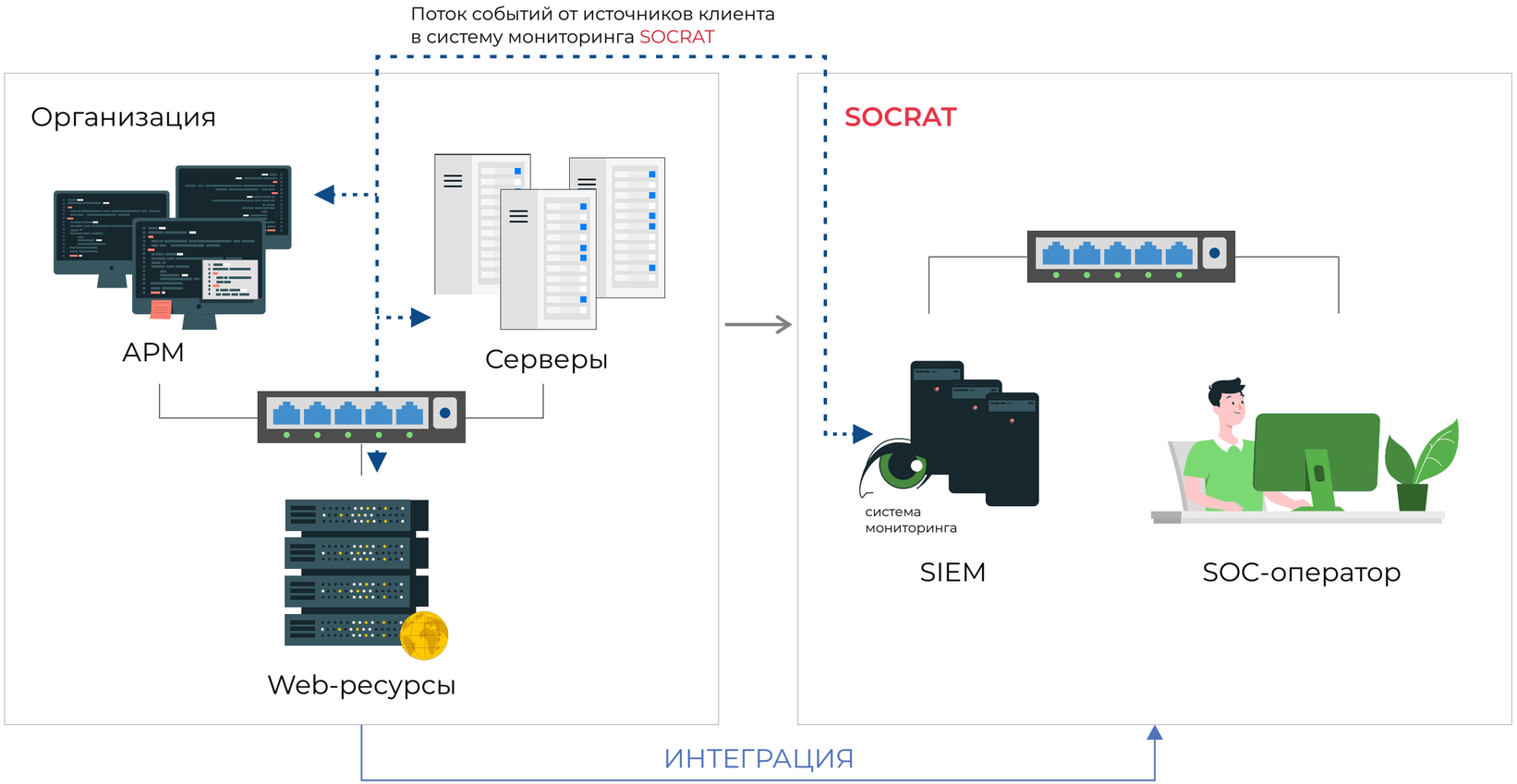
Вариант 3. Интеграция имеющейся в организации системы мониторинга с системой SOCRAT



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

Сервисная модель



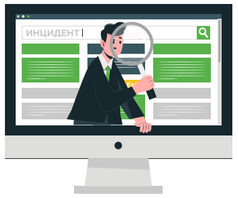
Если у вас нет возможности построить систему мониторинга в своей инфраструктуре, а также нет специалистов для организации непрерывного процесса мониторинга и реагирования на инциденты безопасности, мы предлагаем облегченный вариант подключения

Наша команда при помощи агентов либо безагентным способом подключит ваши источники событий к системе мониторинга в 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?

SOC
RAT

SECURITY
OPERATION
CENTER
RUSSIAN
ANALYTICS
TEAM

SOCRAT – это ваша возможность получить:

Мониторинг инцидентов ИБ в режиме 24/7

Вариативность при подключении к Центру мониторинга

Высокий SLA – моментальное реагирование на инциденты

Индивидуальный подход к потребностям компании
и особенностям ее инфраструктуры

Доступность по цене

КТО МЫ

Компания КСБ-СОФТ – системный интегратор в сфере информационной безопасности и импортозамещения информационных технологий

Анализ уязвимостей
и тестирование
на проникновение

Аудит
информационной
безопасности

Мониторинг
и реагирование
на инциденты ИБ

Обеспечение
безопасности
КИИ и АСУ ТП

Консалтинг по безопас-
ной разработке
и сертификации СЗИ

Защита информации
в ГИС и ИСПДн

Наш вклад в кибербезопасность

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

Созданный в соответствии с передовыми практиками цикл безопасной разработки

Активная деятельность в российском комьюнити безопасной разработки

Наши клиенты – государственные и коммерческие организации в 80 регионах России

На сегодня в портфолио компании 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 АТАКАМ

КСБ-СОФТ

8 800 3333-872

+7 (8352) 322-322

info@ksb-soft.ru

КАНАЛ
«МНЕНИЕ ИНТЕГРАТОРА»

ПОДКАСТ
«SOCRAT ЗА СТЕКЛОМ»

САЙТ
КОМПАНИИ