КСБ-СОФТ

SOCRAT

SECURITY
OPERATION
CENTER
RUSSIAN
ANALYTICS
TEAM

ЦЕНТР МОНИТОРИНГА И РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (SOC)

ЗАЧЕМ ЗАЩИЩАТЬ ИНФОРМАЦИЮ

Мониторинг и реагирование на инциденты информационной безопасности – не только мера для обеспечения практической безопасности, но и одно из требований госрегуляторов

С каждым годом информационная безопасность как отрасль приобретает особое значение, в том числе и на государственном уровне

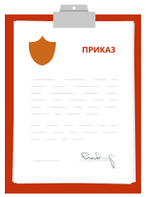
Ежегодно ФСТЭК России проводит проверки значимых объектов КИИ и выявляет нарушения

Сегодня проверки регулятора становятся все более практическими и перестают быть простым пересчетом выполненных на бумаге требований

Помимо требований регуляторов, информационная безопасность является необходимостью, так как интерес злоумышленников к ресурсам российских организаций (как государственных, так и коммерческих) продолжает расти, что заметно на примере успешных атак

Приказ ФСТЭК №17 *
о требованиях к защите информации в ГИС

№ 149-ФЗ
о защите информации



Приказ ФСТЭК №239
о требованиях к защите объектов КИИ

№ 152-ФЗ
о персональных данных

ГОСТ Р 59547-2021
общие положения о мониторинге информационной безопасности

№ 187-ФЗ
о безопасности КИИ

* С учетом возможных изменений

КАК ЗАЩИЩАТЬ ИНФОРМАЦИЮ

Эффективная система защиты информации должна выполнять два условия: быть непрерывной и быть комплексной

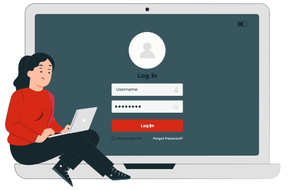
Построение системы защиты нужно начать с оценки рисков для организации, определения состава защищаемых ресурсов и их текущей защищенности

Чтобы система защиты была эффективной и могла противодействовать актуальным угрозам безопасности необходимо внедрять и поддерживать как ИТ, так и ИБ процессы

ЧТО НУЖНО ДЕЛАТЬ

- Периодически проводить инвентаризацию активов как внутренних, так и внешних
- Повышать осведомленность сотрудников организации
- Периодически выявлять и устранять недочеты безопасности
- Своевременно устанавливать обновления на ПО и ОС
- Обеспечить мониторинг событий информационной безопасности и реагирования на инциденты

Хищение конфиденциальной информации



Нарушение доступности ресурсов

Остановка деятельности

Финансовые и репутационные риски

ЧТО ТАКОЕ ЦЕНТР МОНИТОРИНГА

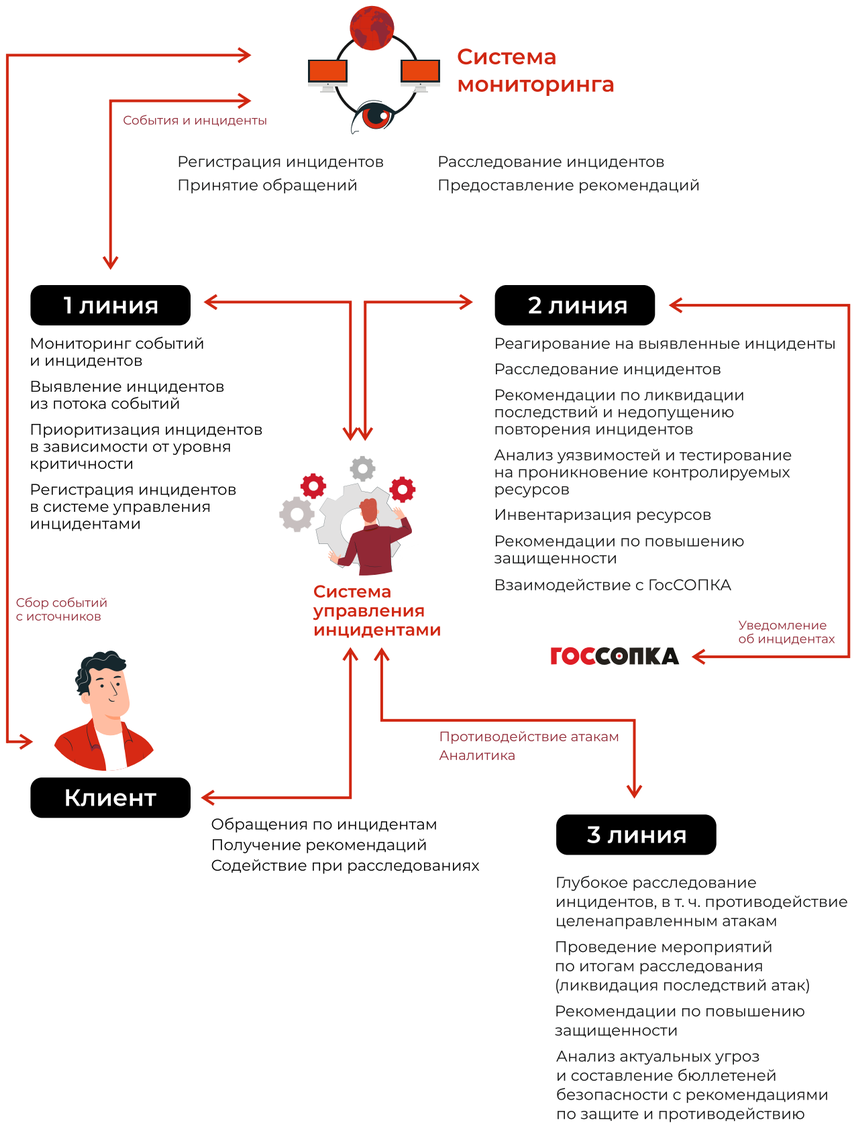


Схема работы Центра мониторинга

ЦЕНТР МОНИТОРИНГА – ЭТО ЛЮДИ, ПРОЦЕССЫ И ТЕХНОЛОГИИ

Специалисты SOC анализируют события информационной безопасности от различных источников: рабочие места, серверы, средства защиты и т.д.

На основе анализа SOC-специалисты выявляют события, способные негативно повлиять на защищаемую инфраструктуру, и бизнес-процессы. Затем их задача — уведомить ответственное лицо, выдать рекомендации и помочь их применить

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

SOCRAT

SECURITY
OPERATION
CENTER
RUSSIAN
ANALYTICS
TEAM

ЦЕНТР МОНИТОРИНГА И РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ КОМПАНИИ КСБ-СОФТ

НЕПРЕРЫВНАЯ ЗАЩИТА ОРГАНИЗАЦИЙ
ОТ УГРОЗ БЕЗОПАСНОСТИ

- Мониторинг 24/7
- Взаимодействие с ГосСОПКА
- Анализ уязвимостей
- Тестирование на проникновение
- Киберучения совместно с МГТУ им. Баумана

КАК ЗАЩИТИТЬСЯ И ВЫПОЛНИТЬ ТРЕБОВАНИЯ РЕГУЛЯТОРОВ

Подключение к SOCRAT – это возможность...

- **Выполнять** требования законодательства
- **Обеспечить** непрерывный контроль безопасности инфраструктуры
- **Осуществлять** взаимодействие с ГосСОПКА
- **Обеспечить** постоянное выявление уязвимостей в прикладном и системном программном обеспечении
- **Получать** поддержку по любым вопросам информационной безопасности

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

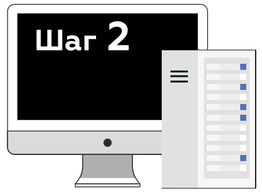
КАК SOCRAT РЕАГИРУЕТ НА ИНЦИДЕНТЫ

1 SOC-специалисты
просматривают события безопасности

Событие оказалось потенциально опасным?

НЕТ

ДА

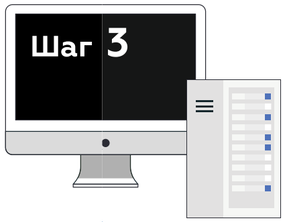


2 SOC-специалисты
проводят первичный анализ событий безопасности

SOC-специалисты заподозрили наличие инцидента?

НЕТ

ДА

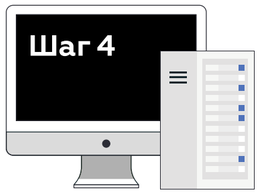


3 SOC-специалисты
создают карточку инцидента
уведомляют ответственное лицо в организации об инциденте

Организация подтвердила инцидент?

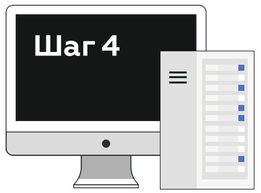
НЕТ

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

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
ПАКЕТ «ГосСОПКА»	Разработка рабочей документации Передача информации об инцидентах в ГосСОПКА Получение от НКЦКИ рекомендаций и направление их в контролируемую организацию

РЕКОМЕНДОВАННЫЕ СХЕМЫ ПОДКЛЮЧЕНИЯ

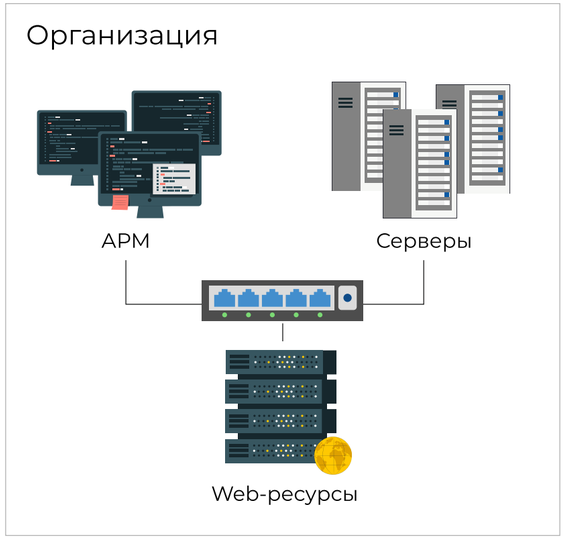
РОИВ/ФОИВ	**БАЗОВЫЙ ПАКЕТ «КОНТРОЛЬ»** **ПАКЕТ «ПРЕДУПРЕЖДЕНИЕ»**
СУБЪЕКТЫ КИИ	**БАЗОВЫЙ ПАКЕТ «КОНТРОЛЬ»** **ПАКЕТ «ПРЕДУПРЕЖДЕНИЕ»** **ПАКЕТ «ГосСОПКА»**
КОММЕРЧЕСКИЕ ОРГАНИЗАЦИИ	**БАЗОВЫЙ ПАКЕТ «КОНТРОЛЬ»** **ПАКЕТ «ПРЕДУПРЕЖДЕНИЕ»** **ПАКЕТ «РАССЛЕДОВАНИЕ»**

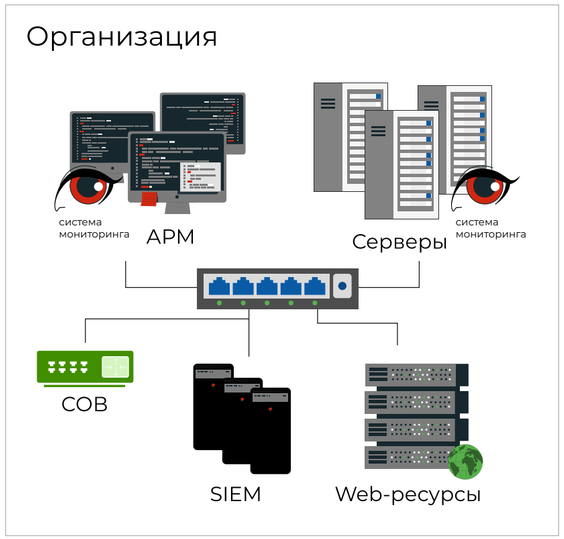
ВАРИАНТЫ ПОДКЛЮЧЕНИЯ К ЦЕНТРУ МОНИТОРИНГА SOCRAT

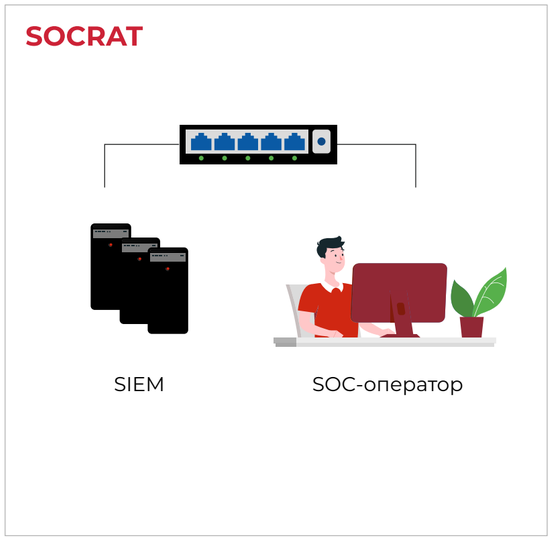
ВАРИАНТ 1. Построение системы мониторинга в организации

Команда SOCRAT поможет с проектированием системы мониторинга, приобретением и внедрением, а также с настройкой и подключением источников событий

Затем мы проведем интеграцию построенной системы мониторинга с системой SOCRAT для обеспечения мониторинга реагирования на инциденты информационной безопасности







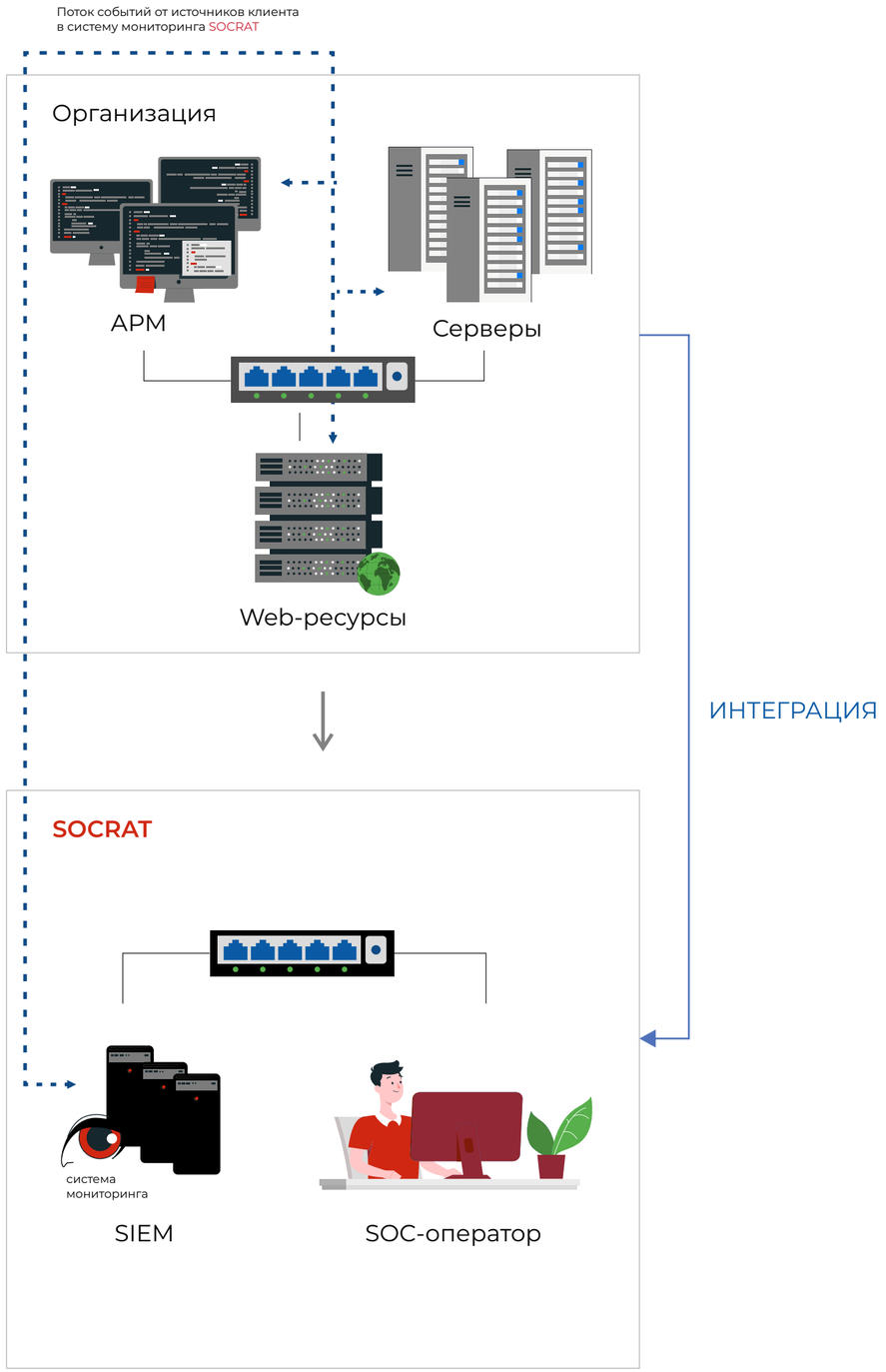
ИНТЕГРАЦИЯ

ВАРИАНТЫ ПОДКЛЮЧЕНИЯ К ЦЕНТРУ МОНИТОРИНГА SOCRAT

ВАРИАНТ 2. SOC по сервисной модели (SOC-as-Service)

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 подключиться к SOCRAT по сервисной модели

Команда SOCRAT поможет организовать мониторинг при помощи своей системы мониторинга



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

Обеспечение непрерывной
безопасности

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

Взаимодействие с НКЦКИ
направление сведений об инцидентах ГосСОПКА

Удобное и оперативное взаимодействие
взаимодействие через удобный
и функциональный сервис

Личная команда ИБ
консультация по любым вопросам ИБ, в том числе
при прохождении проверок регуляторов

КОМПАНИЯ «КСБ-СОФТ»

Системный интегратор в сфере информационной безопасности и импортозамещения информационных технологий

Мониторинг и реагирование
на инциденты ИБ

Анализ уязвимостей и тестирование
на проникновение

Консалтинг по безопасной
разработке и сертификации СЗИ

Аудит информационной
безопасности

Обеспечение безопасности
КИИ и АСУ ТП

Оценка показателя состояния
технической защиты информации
и обеспечения безопасности ЗОКИИ

НАШ ВКЛАД В КИБЕРБЕЗОПАСНОСТЬ

- Защита значимых объектов КИИ РФ
- 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 сообществе по безопасной разработке

Наши клиенты – государственные и коммерческие организации в 80 регионах Российской Федерации

На сегодня в портфолио компании более 6000 проектов разной степени сложности, полученный опыт в которых помогает нам подбирать эффективные решения для защиты информационных ресурсов наших клиентов

ПИЛОТНОЕ ПОДКЛЮЧЕНИЕ

Вы можете бесплатно оценить качество предоставляемых услуг на вашей инфраструктуре

Закажите пилотное подключение к центру мониторинга SOCRAT

Подробнее ознакомиться с нашей экспертизой можно на сайте ksb-soft.ru

Вебинары

Блог

Кейсы

SOCRAT

SECURITY
OPERATION
CENTER
RUSSIAN
ANALYTICS
TEAM

SOCRAT – ЦЕНТР ПРОТИВОДЕЙСТВИЯ КИБЕРАТАКАМ

КСБ-СОФТ

КОНТАКТЫ

8 800 3333-872
info@ksb-soft.ru
ksb-soft.ru