КСБ-СОФТ

SOCRAT

SECURITY
OPERATION
CENTER
RUSSIAN
ANALYTICS
TEAM

ЦЕНТР МОНИТОРИНГА И РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (SOC)

ЗАЧЕМ ЗАЩИЩАТЬ ИНФОРМАЦИЮ

**Меняется как ландшафт угроз,
так и регуляторные меры по защите информации.
Мониторинг и реагирование на инциденты ИБ –
практическая мера безопасности, соответствующая
требованиям НПА и снижающая бизнес-риски.**

СНИЖЕНИЕ БИЗНЕС-РИСКОВ

**Минимизация финансовых
и репутационных рисков:**

- Простой производства и недополученная прибыль.
- Непредвиденные затраты на восстановление работы.
- Штрафы и пени из-за неисполнения контрактов или утечки ПДн (до 3% от прибыли за предыдущий год, но не менее 20 млн рублей).

Своевременное выявление и реагирование на угрозы, способные привести к нарушению бизнес-процессов и к их непрерывности.

Мера, которую могут предъявить заказчики для работы с ними, включая государственные контракты.

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ РЕГУЛЯТОРОВ

№ 149-ФЗ
«О защите информации»

Приказ ФСТЭК № 117
«О требованиях к защите информации в ГИС»

№ 152-ФЗ
«О персональных данных»

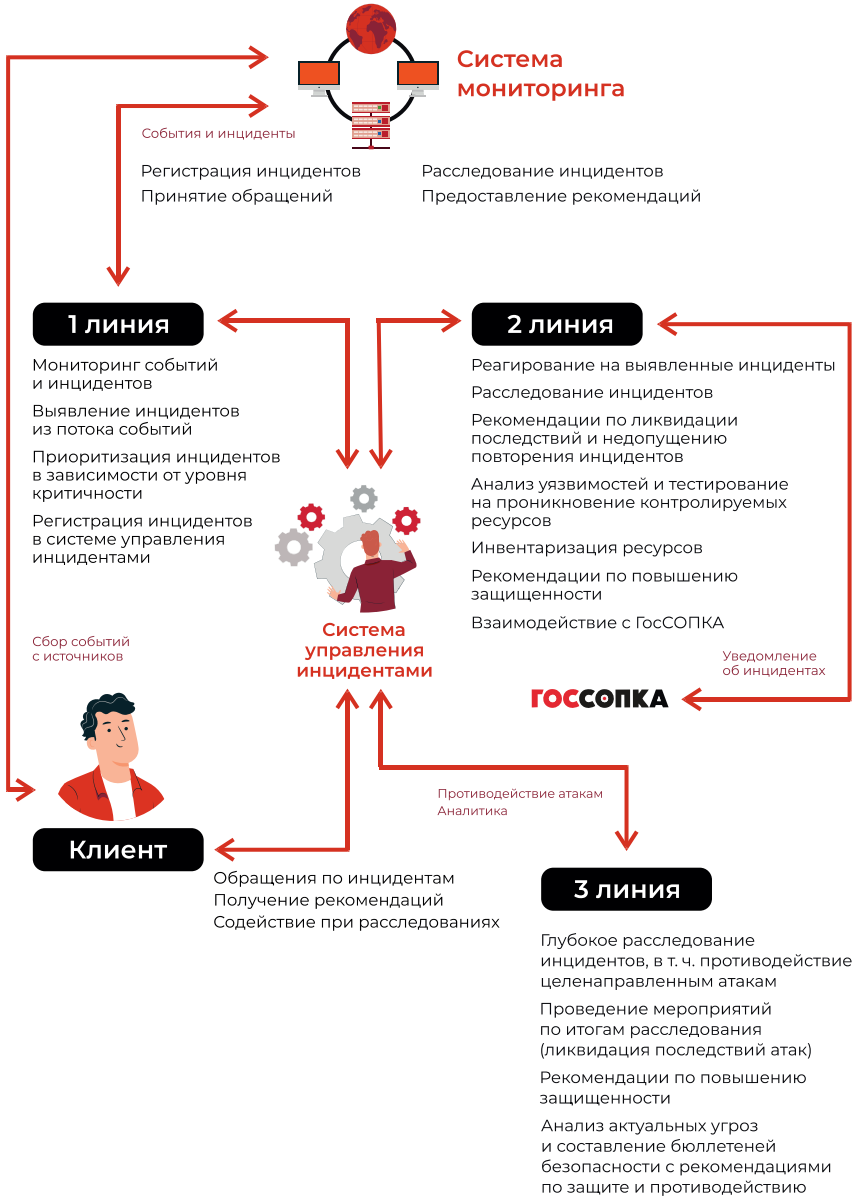
Приказ ФСТЭК № 239
«О требованиях к защите объектов КИИ»

№ 187-ФЗ
«О безопасности КИИ»

ГОСТ Р 59547-2021
общие положения о мониторинге информационной безопасности

**Приказы ФСБ России
№ 546, 547, 548**
взаимодействие с НКЦКИ

ЦЕНТР МОНИТОРИНГА – ЭТО НЕ ТОЛЬКО МОНИТОРИНГ



ЦЕНТР МОНИТОРИНГА – ЭТО ЛЮДИ, ПРОЦЕССЫ И ТЕХНОЛОГИИ

Аналитики осуществляют непрерывный контроль за безопасностью защищаемых ресурсов и анализируют тренды угроз. Выявляют атаки и инциденты ИБ. Взаимодействуют с ответственными лицами и НКЦКИ.

Процессы – это четко определенные, документированные и постоянно совершенствуемые рабочие процедуры для обнаружения, классификации, исследования и нейтрализации инцидентов безопасности.

Технологии – это специализированные системы сбора данных (SIEM), платформы анализа угроз, инструменты для расследования инцидентов, системы обнаружения вторжений (IDS/IPS), решения для управления информацией и событиями безопасности.

ЦЕНТР МОНИТОРИНГА – ЭТО НЕ ТОЛЬКО МОНИТОРИНГ

Аналитики SOCRAT помимо мониторинга событий безопасности и анализа подозрений на атаки и инциденты, имеют смены развития, в рамках которых:

- Повышают свой **уровень знаний** и компетенций, тренируясь на специализированных площадках.
- **Развивают** направления Threat Intelligence, Threat Hunting, Malware Analyst, Revers Engineering, Detection Engineering, DFIR.
- **Изучают** передовые продукты: SIEM, VM, EDR, SOAR, IRP, SandBox и другие классы решений.
- **Разрабатывают** инструменты автоматизации.
- **Дорабатывают** правила для системы мониторинга.
- Проходят **обучающие курсы**, включая вендорские курсы по продуктам, используемым при мониторинге и реагировании.

ЛЮДИ



Специалисты центра мониторинга SOCRAT имеют опыт работы как в коммерческих организациях, так и в органах исполнительной власти.

ЦЕНТР МОНИТОРИНГА – ЭТО НЕ ТОЛЬКО МОНИТОРИНГ

Процессы выстраиваются на основании лучших практик и требований регулятора, в том числе ГОСТ Р 59547-2021 и методических рекомендаций НКЦКИ.

- **Мониторинг** унифицирован внутренним стеком инструментов и включает интеграцию с TIP, а также работу с базой отработанных атак и инцидентов.
- **Реагирование** реализовано при помощи IRP-системы и предусматривает единый формат карточек атак и инцидентов, а также сценарии реагирования.
- **Контроль** включает ежемесячный сбор статистики, выполнение SLA и схему перепроверки карточек атак и инцидентов.
- **Развитие** направлений реализуется через закрепление ответственного лица за каждым направлением.
- **Администрирование** обеспечивает контроль за обновлением баз правил и версий инструментов, а также оперативное восстановление работоспособности в случае ее нарушения.
- **Актуализация** правил системы мониторинга охватывает настройку корреляционных правил на основе информации от регуляторов, требований заказчиков и трендовых угроз.
- **Взаимодействие** с ответственным лицом заказчика и НКЦКИ реализовано при помощи IRP-системы.

ПРОЦЕССЫ



ЦЕНТР МОНИТОРИНГА – ЭТО НЕ ТОЛЬКО МОНИТОРИНГ

Центр мониторинга использует различные инструменты и системы, чтобы предоставлять качественные и экспертные услуги. В SOCRAT применяются решения, имеющие необходимые сертификаты ФСТЭК России и ФСБ России, а также решения из РОПО.

САМОПИСНЫЕ и open source инструменты и утилиты.

Инструменты сбора образцов компрометации и их анализа для расследования инцидентов ИБ.

КСБ-СОФТ

ТЕХНОЛОГИИ

ВЕНДОРСКИЕ

SIEM

- MaxPatrol SIEM
- Solar SIEM
- ViPNet TIAS

VM

- MaxPatrol VM

EDR

- MaxPatrol EDR

IRP/SOAR

- АльфаИнциденты

СКЗИ

- ViPNet
- Континент

SandBox

- PT SandBox

TIP/TI-feeds

- 4RAYS (Solar)

ЦЕНТР МОНИТОРИНГА – ЭТО НЕ ТОЛЬКО МОНИТОРИНГ

Функции и направления центра мониторинга: объединение лучших практик и требований регулятора

Внутренний контроль:
- Перепроверка карточек инцидентов
- Соответствие заявленному SLA
- Соответствие внутренним метрикам качества и эффективности

Оценка уровня защищенности:
- Инвентаризация
- Выявление уязвимостей
- Оценка защищенности

Мониторинг и реагирование:
- Сбор событий безопасности с различных источников
- Анализ событий безопасности
- Контроль работоспособности систем
- Информирование об угрозах безопасности и нарушении функционирования
- Подготовка периодических и итоговых отчетов



Экспертиза:
- Получение новых данных об индикаторах компрометации
- Разработка новых или доработка текущих правил систем мониторинга для снижения количества ложно-позитивных сработок и детектирования новых угроз
- Реагирование на инциденты с помощью (EDR/SOAR)
- Расследование инцидентов
- Глубокий анализ подозрительных файлов
- Анализ угроз при помощи Threat Intelligence/Threat Hunting

Взаимодействие с НКЦКИ:
- Включение в свою зону ответственности ресурсов организации-заказчика
- Уведомления в ГосСОПКА

Сопровождение систем мониторинга:
- Обновление экспертных данных
- Обновление компонентов
- Восстановление работоспособности
- Подключение источников событий

Корпоративный центр ГосСОПКА КСБ-СОФТ – ответственность перед регулятором за ваши ресурсы

SOCRAT

SECURITY
OPERATION
CENTER
RUSSIAN
ANALYTICS
TEAM

Мониторинг 24/7

Тестирование на проникновение

Вариативность подключения

Поток данных об актуальных угрозах

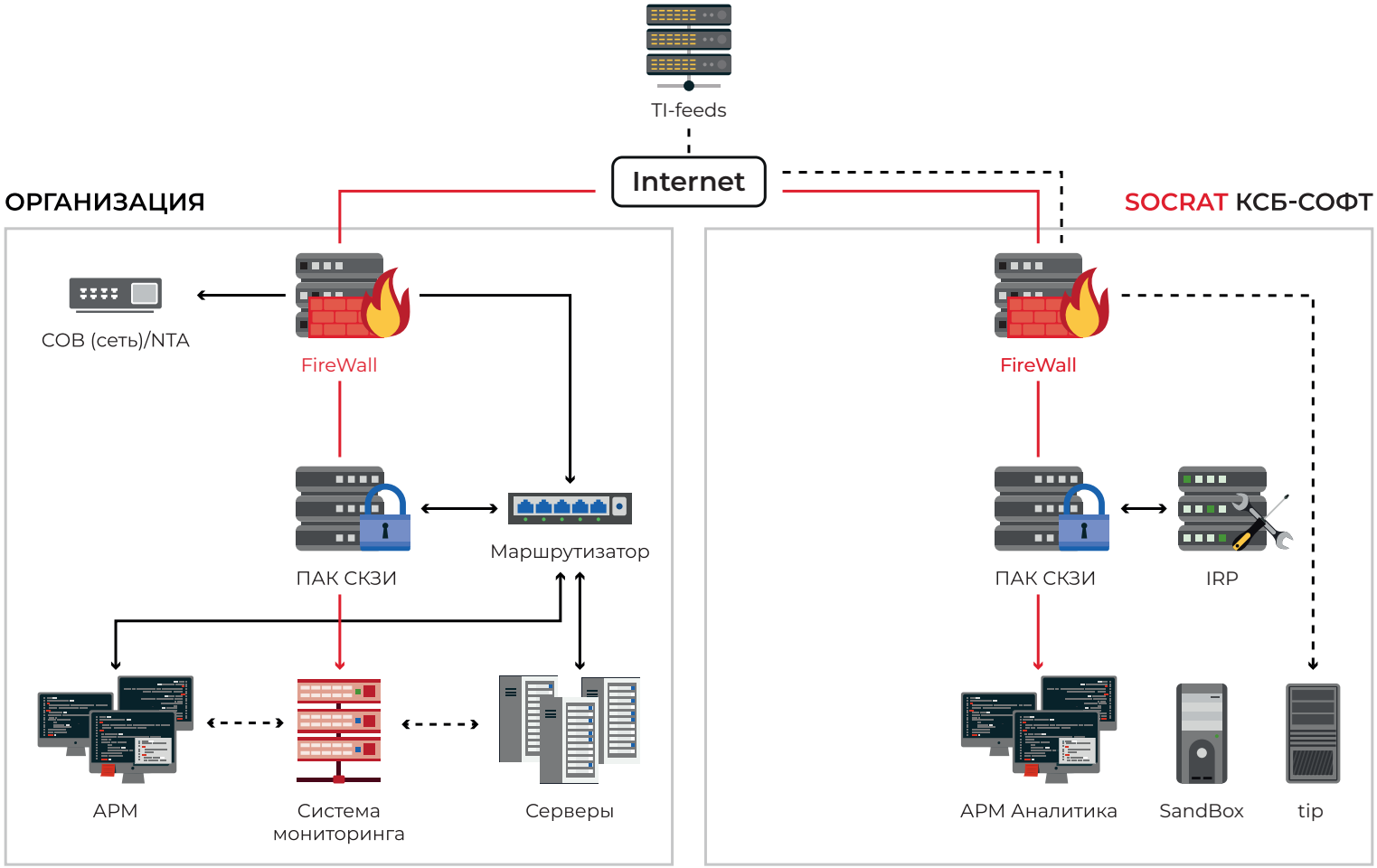
Реагирование

Взаимодействие с ГосСОПКА

Соответствие требованиям регулятора

ВАРИАНТЫ ПОДКЛЮЧЕНИЯ К ЦЕНТРУ МОНИТОРИНГА SOCRAT

ВАРИАНТ 1. ГИБРИД

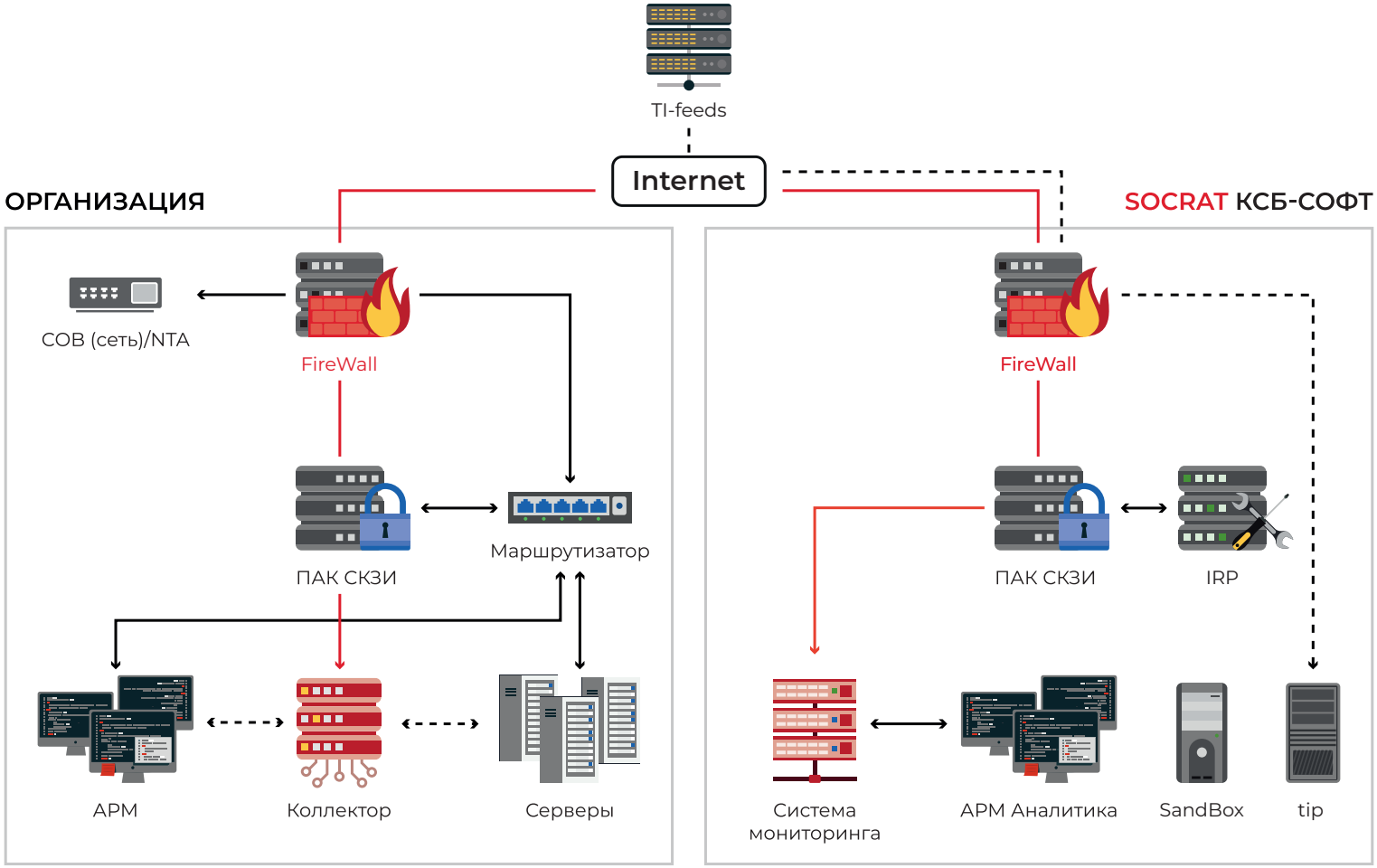


При гибридном варианте система мониторинга находится в вашей инфраструктуре. Аналитики центра мониторинга используют ваши технологии для оказания услуг по мониторингу и реагированию на инциденты.

Если у вас отсутствует система мониторинга, мы в зависимости от ваших целей и задач поможем ее спроектировать, закупить, внедрить, настроить, а также завести источники событий.

ВАРИАНТЫ ПОДКЛЮЧЕНИЯ К ЦЕНТРУ МОНИТОРИНГА SOCRAT

ВАРИАНТ 2. SOC ПО СЕРВИСНОЙ МОДЕЛИ (SOC-AS-SERVICE)



При сервисном варианте система мониторинга предоставляется центром мониторинга. Аналитики внедряют в вашу инфраструктуру необходимые компоненты (потребуются серверные мощности), настраивают, а также помогают с заведением источников событий.

ПАКЕТЫ ПОДКЛЮЧЕНИЯ К SOCRAT

БАЗОВЫЙ ПАКЕТ «КОНТРОЛЬ»	Мониторинг и реагирование на инциденты ИБ (24/7 или 8/5)
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»** **ПАКЕТ «ГосСОПКА»**
СУБЪЕКТЫ КИИ	**БАЗОВЫЙ ПАКЕТ «КОНТРОЛЬ»** **ПАКЕТ «ПРЕДУПРЕЖДЕНИЕ»** **ПАКЕТ «ГосСОПКА»**
КОММЕРЧЕСКИЕ ОРГАНИЗАЦИИ	**БАЗОВЫЙ ПАКЕТ «КОНТРОЛЬ»** **ПАКЕТ «РАССЛЕДОВАНИЕ»**

SOCRAT ДЛЯ ГОССЕГМЕНТА

Мониторинг и реагирования на инциденты информационной безопасности в соответствии с требованиями ФСТЭК России и ФСБ России

ПРИКАЗ ФСТЭК РОССИИ № 117

раздел 3, пп.49

ГОСТ Р 59547-2021

Отчет для отправки во ФСТЭК России

- Анализ событий безопасности
- Контроль (анализ) защищенности
- Анализ и оценка функционирования СЗИ
- Анализ изменения угроз безопасности

раздел 3, х)

Приказы ФСБ России:

- № 547
- № 548

- Непрерывное взаимодействие с ГосСОПКА
- Информирование НКЦКИ о выявленных КА и КИ

РОИВ/ФОИВ

БАЗОВЫЙ ПАКЕТ
«КОНТРОЛЬ»

ПАКЕТ
«ПРЕДУПРЕЖДЕНИЕ»

ПАКЕТ
«ГосСОПКА»

Дополнительно:

Команда КСБ-СОФТ может помочь с проведением комплексных работ по защите ИС:

- разработка ОРД;
- внедрение СЗИ;
- внедрение процессов (например, управление уязвимостями);
- анализ уязвимостей;
- тестирование на проникновение по типовому ТЗ Минцифры;
- аттестации ИС.

Подготовка и помощь при прохождении проверок регуляторов.

Проведение киберучений с отправкой отчета в ГосСОПКА.

SOCRAT ДЛЯ КИИ

ПРИКАЗ ФСТЭК РОССИИ № 239 **ФЗ-187**

Обеспечение безопасности ЗОКИИ

Постоянные мероприятия:

- Мониторинг и анализ зарегистрированных событий
- Реагирование на КИ

Периодические мероприятия:

- Анализ уязвимостей ЗОКИИ

Взаимодействие с ГосСОПКА

Приказы ФСБ России:

- № 546
- № 547
- № 548

- Непрерывное взаимодействие с ГосСОПКА
- Информирование НКЦКИ о выявленных КА и КИ

СУБЪЕКТЫ КИИ

БАЗОВЫЙ ПАКЕТ «КОНТРОЛЬ»

ПАКЕТ «ПРЕДУПРЕЖДЕНИЕ»

ПАКЕТ «ГосСОПКА»

Дополнительно:

Команда КСБ-СОФТ может помочь с проведением комплексных работ по защите КИИ (в том числе АСУ ТП):

- выявление ОКИИ;
- категорирование;
- разработка ОРД;
- внедрение СЗИ.

Подготовка и помощь при прохождении проверок регуляторов.

Помощь с организацией взаимодействия с НКЦКИ с помощью SOCRAT или самостоятельно.

SOCRAT ДЛЯ КОММЕРЧЕСКИХ ОРГАНИЗАЦИЙ

Классический центр мониторинга в случае если госзаказчик предъявляет требования к защите информации (для работы по госконтрактам), в состав которых входит обеспечение мониторинга.

MDR-сервис в случае если требуется организовать непрерывный контроль за защищенностью ключевых ресурсов организации и активное реагирование в случае выявления атак и инцидентов ИБ.

Ценности:

- Круглосуточный мониторинг при поддержке экспертов ЦМ
- Правила корреляции для выявления продвинутых атак
- Поиск вредоносного ПО с помощью YARA-правил
- Данные об актуальных угрозах
- Автоматизированные уведомления
- Автоматизированное реагирование
- Рекомендации по выявленным инцидентам

КОММЕРЧЕСКИЕ ОРГАНИЗАЦИИ

БАЗОВЫЙ ПАКЕТ
«КОНТРОЛЬ»

ПАКЕТ
«РАССЛЕДОВАНИЕ»

Дополнительно:

Команда КСБ-СОФТ поможет с проведением комплексных работ по защите информации, включая:

- разработку организационно-распорядительной документации;
- внедрение систем защиты;
- проведение анализа уязвимостей и тестирования на проникновение (тестирование веб-приложений, внешнего и внутреннего периметра, социальная инженерия).

SOCRAT ДЛЯ ВСЕХ

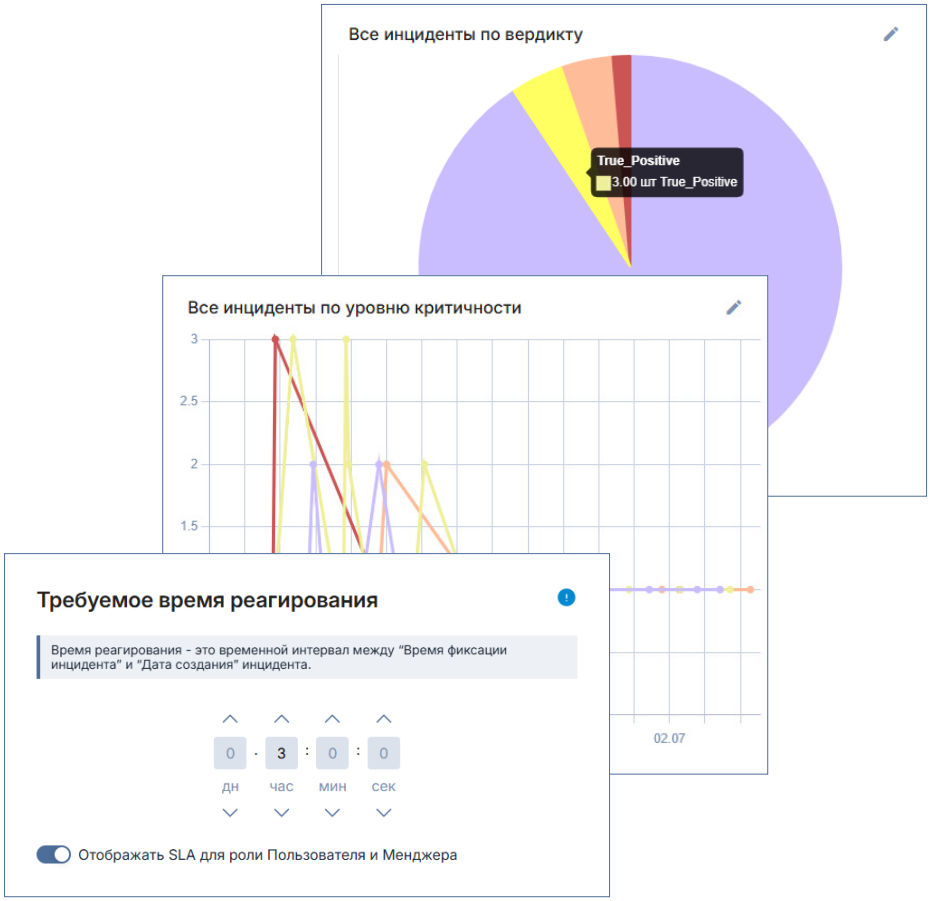
	БАЗОВЫЙ ПАКЕТ «КОНТРОЛЬ»	ПАКЕТ «ГосСОПКА»	ПАКЕТ «ПРЕДУПРЕЖДЕНИЕ»	ПАКЕТ «РАССЛЕДОВАНИЕ»
ГИБРИД	РОИВ/ФОИВ Субъекты КИИ Коммерческие организации	РОИВ/ФОИВ Субъекты КИИ Коммерческие организации (работающие по госконтрактам и являющиеся подрядчиками для госорганов)	РОИВ/ФОИВ Субъекты КИИ	Коммерческие организации
СЕРВИС	Подведомственные организации РОИВ/ФОИВ Субъекты КИИ Коммерческие организации	Подведомственные организации РОИВ/ФОИВ Субъекты КИИ Коммерческие организации (работающие по госконтрактам и являющиеся подрядчиками для госорганов)	РОИВ/ФОИВ Субъекты КИИ	Коммерческие организации

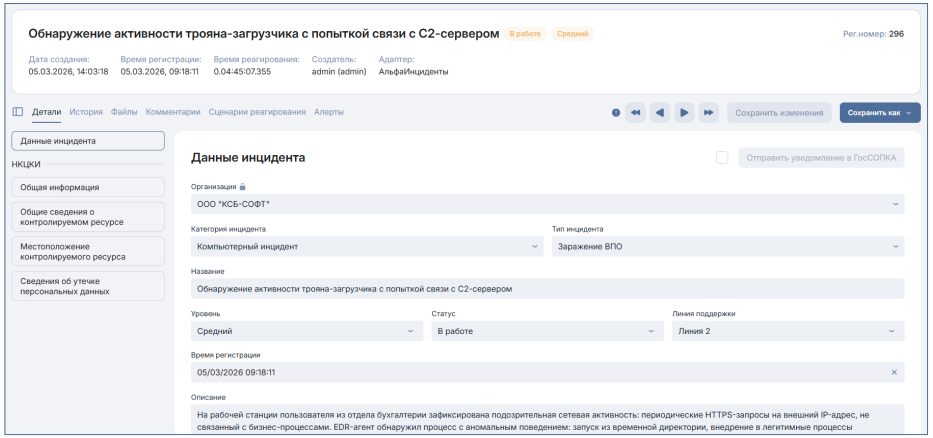
ВЗАИМОДЕЙСТВИЕ SOCRAT

Взаимодействие организуется при помощи IRP-системы АльфаИнциденты.

IRP-система позволяет выстроить процесс управления инцидентами ИБ за счет возможностей:

- **получать уведомления** о выявленных компьютерных атаках и инцидентах с их описанием и рекомендациями по устранению причин и последствий
- при возникновении вопросов либо сложностей при выполнении рекомендаций можно **взаимодействовать** со специалистами SOCRAT **через встроенный чат**
- **выгружать карточки** компьютерных атак и компьютерных инцидентов **в формате**, установленном **НКЦКИ** с целью дальнейшей отправки в ГосСОПКА (в случае взаимодействия с регулятором по электронной почте)
- **выгружать список** всех заведенных **компьютерных атак и инцидентов** в виде таблицы для формирования статистики за выбранный период
- **создавать отчеты** за выбранный период
- **задавать** минимально необходимое время реагирования и **отслеживать выполнение SLA**





АльфаИнциденты (входит в РОПО, реестровая запись №28691 от 09.07.2025) IRP-система разработанная под запросы специалистов центра мониторинга с учетом внутренних процессов SOCRAT

ЧТО В ИТОГЕ?



Обеспечение непрерывной безопасности инфраструктуры (информационных систем)



Своевременное реагирование и противодействие инцидентам информационной безопасности



Расследование инцидентов безопасности и помощь в устранении их последствий



Соответствие законодательным требованиям



Оценка защищенности (тестирование на проникновение)

ПОЧЕМУ ИМЕННО МЫ?

Мониторинг 24/7
круглосуточный мониторинг инцидентов безопасности аналитиками SOC

Настраиваемый SLA
Реагирование в соответствии с требованиями регулятора, либо вашими предпочтениями

Ключевые технологии и экспертиза SOCRAT
Работаем с различными вендорами SIEM и EDR. Используем в работе SandBox, TIP, IRP и другие решения. TI-feeds от одного из крупнейших поставщиков экспертизы

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

Взаимодействие с НКЦКИ
Являемся Корпоративным центром ГосСОПКА. Являемся лицензиатом ФСТЭК России и ФСБ России

Удобное и оперативное взаимодействие
Взаимодействие через личный кабинет (IRP-система разработанная под требования SOCRAT), включающий ИИ-модули

КСБ-СОФТ – ваша 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



Внедрение процессов
безопасной разработки



Аудит информационной
безопасности



Обеспечение безопасности
КИИ и АСУ ТП



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

ПИЛОТНОЕ ПОДКЛЮЧЕНИЕ

Сомневаетесь?

Организуем пилотный проект **SOCRAT**

- Внедрение системы мониторинга
- Контроль состояния защищенности
- Выявление угроз безопасности и предоставление рекомендаций по их устранению
- Обнаружение следов компрометации
- Итоговый отчет

Быстрый переход от пилотного проекта к реальному

Вы можете более подробно ознакомиться с нашей экспертизой:

Вебинары

Блог

Кейсы



КСБ-СОФТ

КОНТАКТЫ

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