КСБ-СОФТ

117 приказ ФСТЭК России.
Мониторинг и реагирование с точки зрения регулятора

- **Алексей Федотов**
  Продуктовый менеджер SOCRAT
- **Александр Кирий**
  Руководитель центра мониторинга SOCRAT

Время вебинара ~ 50 мин

Обменивайтесь сообщениями
во вкладке «Чат»

Запись вебинара направим всем
участникам на указанный
при регистрации e-mail
в течение 2-3 рабочих дней

Задавайте вопросы во вкладке
«Вопросы»

Среди заданных вами вопросов, каждый Эксперт выберет лучший, на его взгляд, вопрос, и мы наградим 2-х авторов фирменным мерчем!

КСБ-СОФТ

Системный интегратор в сфере информационной безопасности и импортозамещения информационных технологий

Входим в ГК «Кейсистемс»

Лицензиат ФСТЭК России

Лицензиат ФСБ России

80+

регионов внедрения

4000+

реализованных проектов

Новые требования к защите информации в ГИС и иных ИС ОГВ

Приказ ФСТЭК России от 11 апреля 2025 г. № 117. Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений

Вступает в силу 01 марта 2026 г.

Приказ распространяется на:

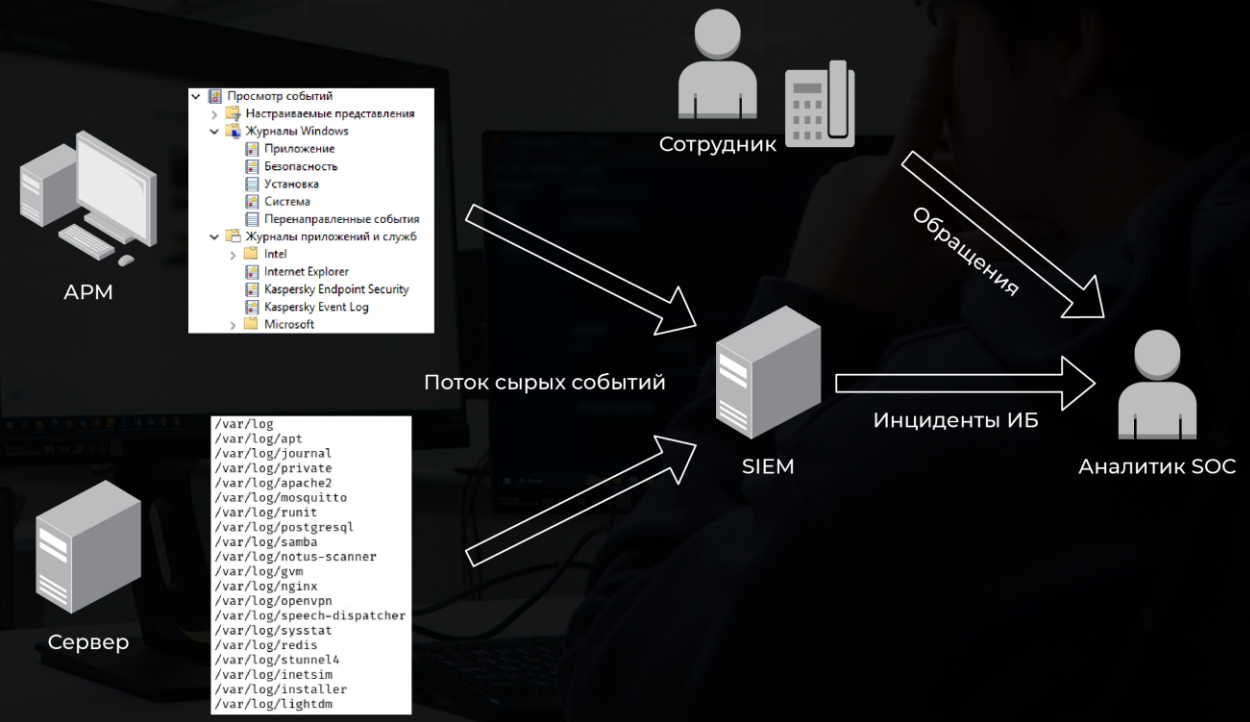
Государственные органы, государственные унитарные предприятия, государственные учреждения

Организации-подрядчики государственных органов, имеющие подключение к ИС

Как организовать сбор событий безопасности?

Приказ № 117, раздел 3, пп.49;
ГОСТ Р 59547-2021, раздел 4, п.4.1

- Внедрить SIEM-систему;
- Собирать события с узлов ИС: ОС, ПО, СЗИ и прочее;
- Принимать обращения от сотрудников организации;
- Информировать ответственного.

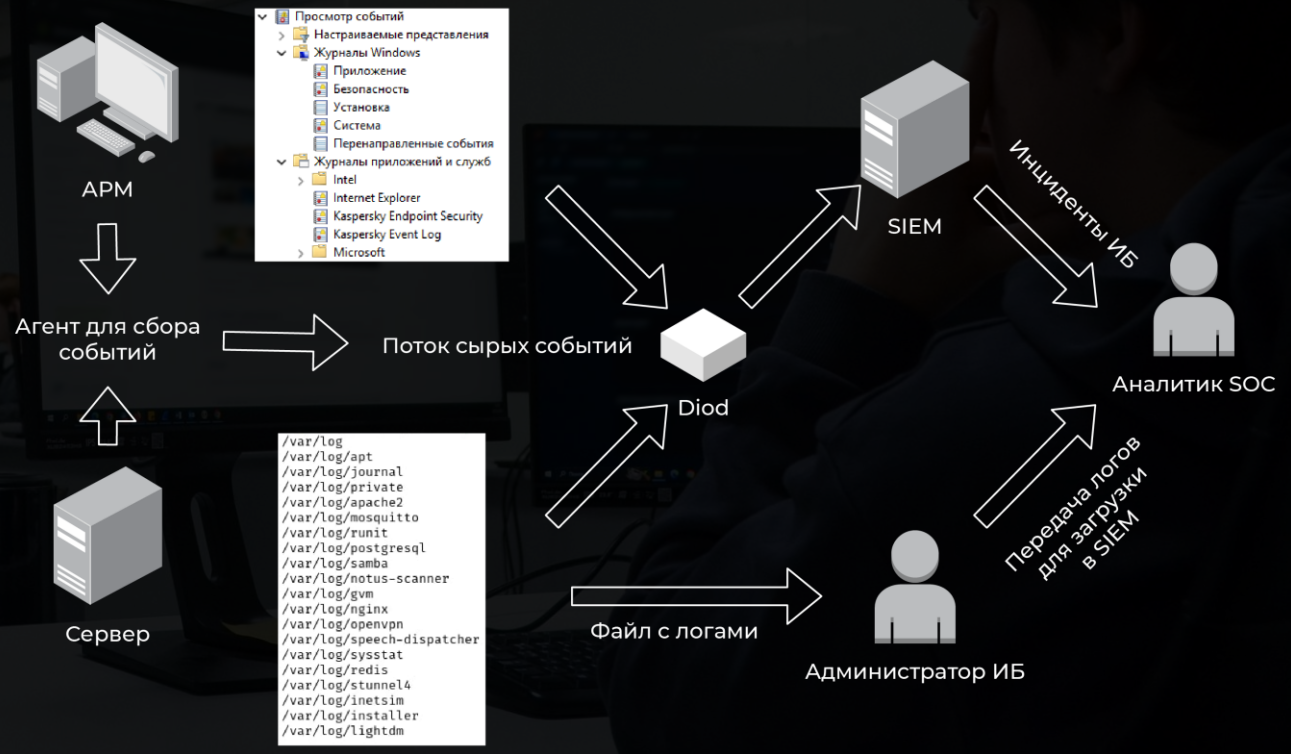


Как организовать сбор событий безопасности?

Приказ № 117, раздел 3, пп.49

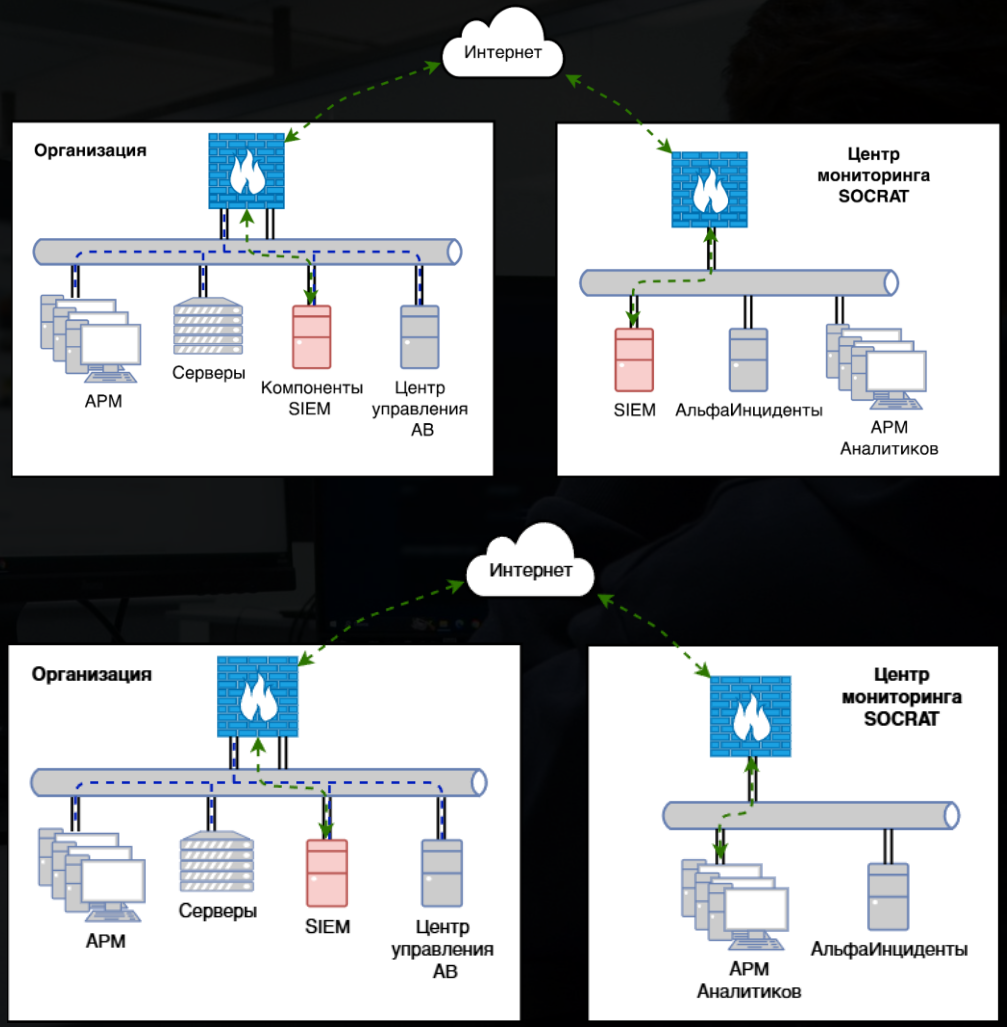
Для изолированных и локальных ИС:

- Агентский сбор событий и их передача через средство однонаправленного потока данных
- Сбор событий через агент SIEM с последующей загрузкой в SIEM



Как реализовано в SOCRAT?

- Проектирование архитектуры
- Внедрение SIEM-системы:
  - On-premise
  - MSSP
- Заведение источников событий совместно с заказчиком
- Приема обращений и взаимодействие через АльфаИнциденты



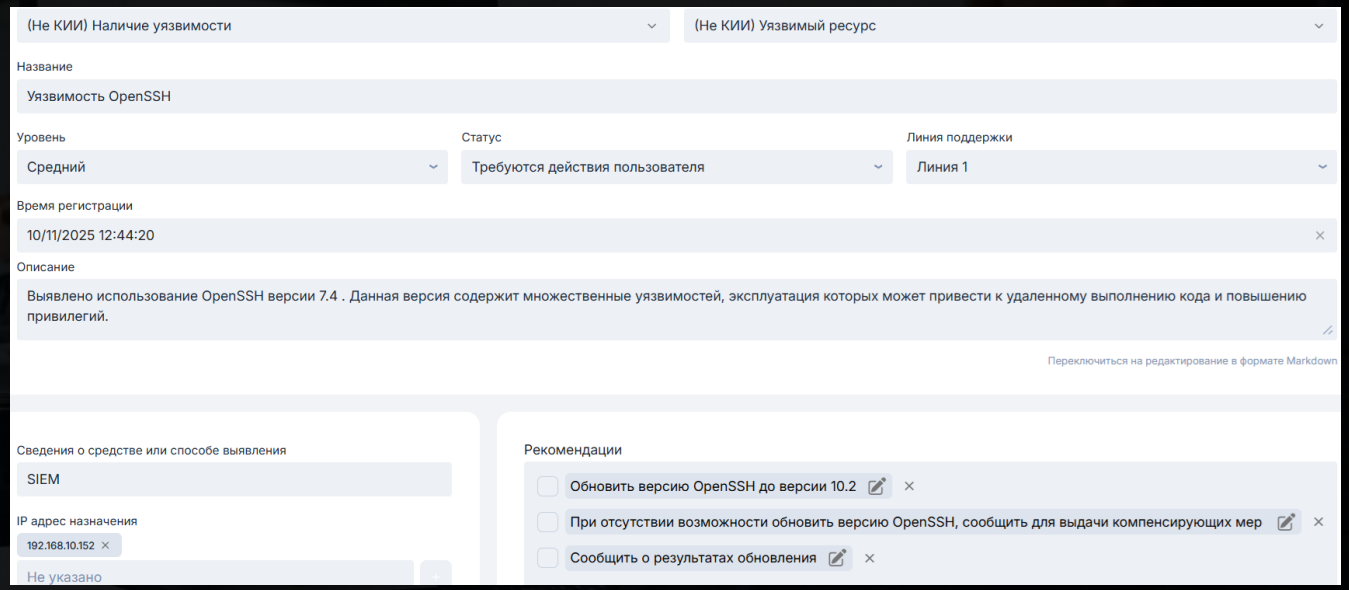
Что контролировать?

ГОСТ Р 59547-2021, раздел 4, п.4.2 а)

- Аномалии в поведении ИС;
- Подозрительный сетевой трафик;
- Подозрительные действия пользователей;
- Нарушение политик безопасности;
- Срабатывание средств защиты;
- Информировать ответственного.

Как реализовано в SOCRAT?

- В процессе мониторинга фиксируются:
  - Нарушения политик безопасности;
  - Уязвимости ПО и ОС;
  - Подозрительные действия пользователей;
  - Реакция систем защиты.
- По итогу фиксации создаются карточки инцидентов и направляются ответственному лицу.



Как анализировать?

ГОСТ Р 59547-2021, раздел 4, п.4.2 г)

Поток событий обогащать:

- данными об уязвимостях;
- идентификаторами компрометации.

В процессе мониторинга:

- дорабатывать правила;
- фильтровать ложные инциденты;
- фиксировать нарушения политик ИБ.

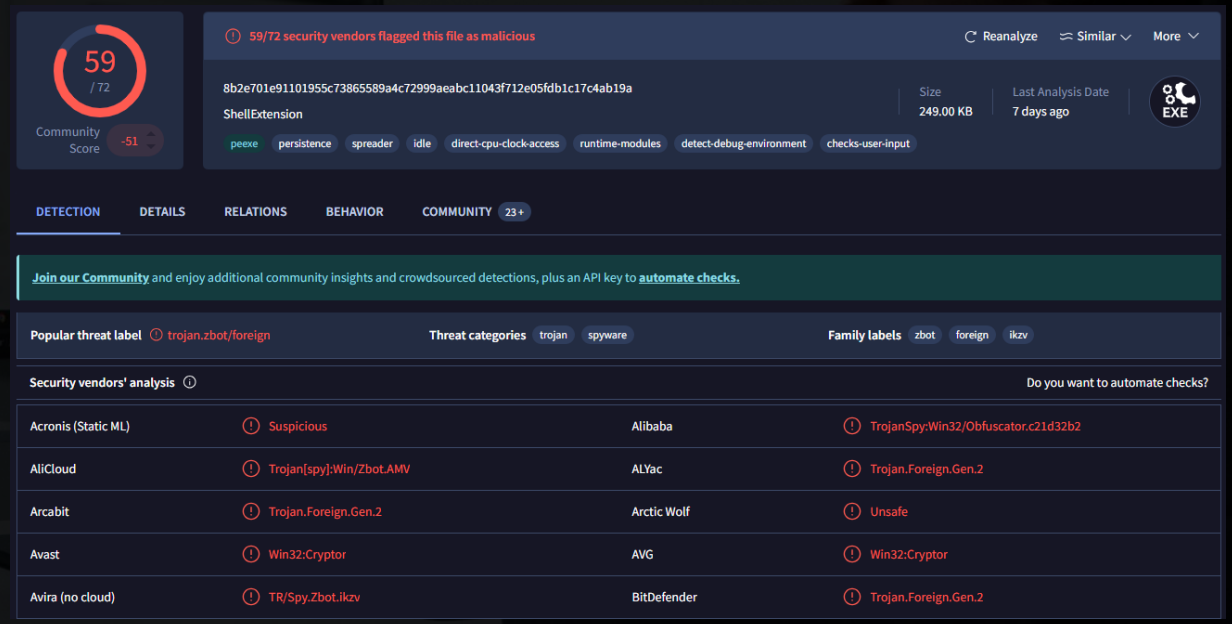
Как реализовано в SOCRAT?

При выявлении подозрения на инцидент, аналитик:

- Проверяет, был ли подобный инцидент;
- Сверяется с информацией об инфраструктуре и результатами анализа уязвимостей;
- Собирает информацию из открытых источников;
- Проверяет совпадение по базам с идентификаторами компрометации.

Для ложных инцидентов добавляются исключения

Инциденты вносятся в базу инцидентов в виде кейса



Как снизить вероятность инцидента ИБ?

ГОСТ Р 59547-2021, раздел 4, п.4.2 б)

Контроль (анализ) защищенности:

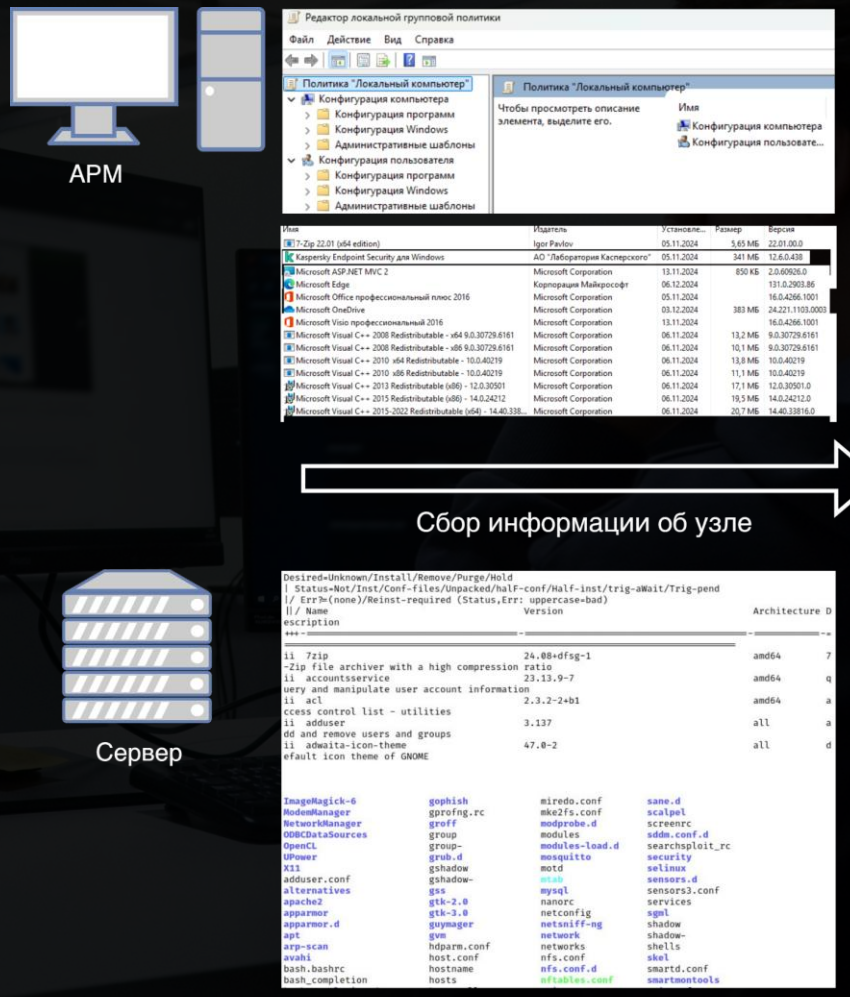
- Выявлять и описывать уязвимости
- Контролировать установку обновлений;
- Проводить инвентаризацию;
- Контролировать настройку ПО и СЗИ в соответствии с политиками ИБ;
- Информировать ответственного.

Как реализовано в SOCRAT?

В рамках одного из пакетов услуг периодически проводятся:

- Инвентаризация;
- Анализ уязвимостей;
- Тестирование на проникновение.

Предоставляется услуга по управлению уязвимостями.

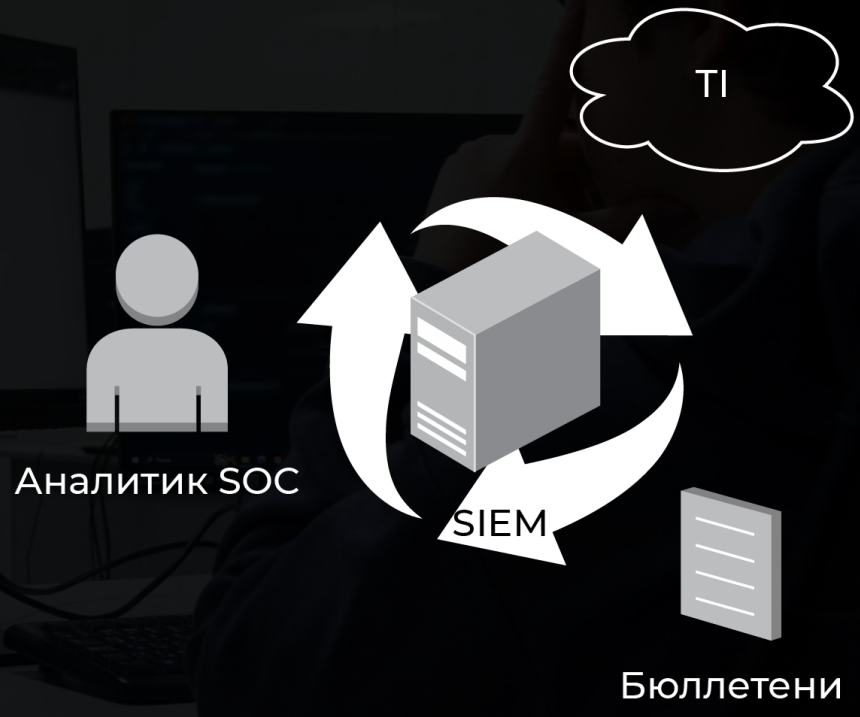


Как поддерживать актуальность?

ГОСТ Р 59547-2021, раздел 4, п.4.2 г)

Анализ угроз:

- Внесение в SIEM идентификаторов компрометации от TI-платформы, рассылки регуляторов и не основе анализа угроз аналитиков;
- Выявление аномалий и актуализация правил в SIEM
- Формировать предложения по расширению зоны действия мониторинга (на основе недостаточной информации и изменений ландшафта угроз)

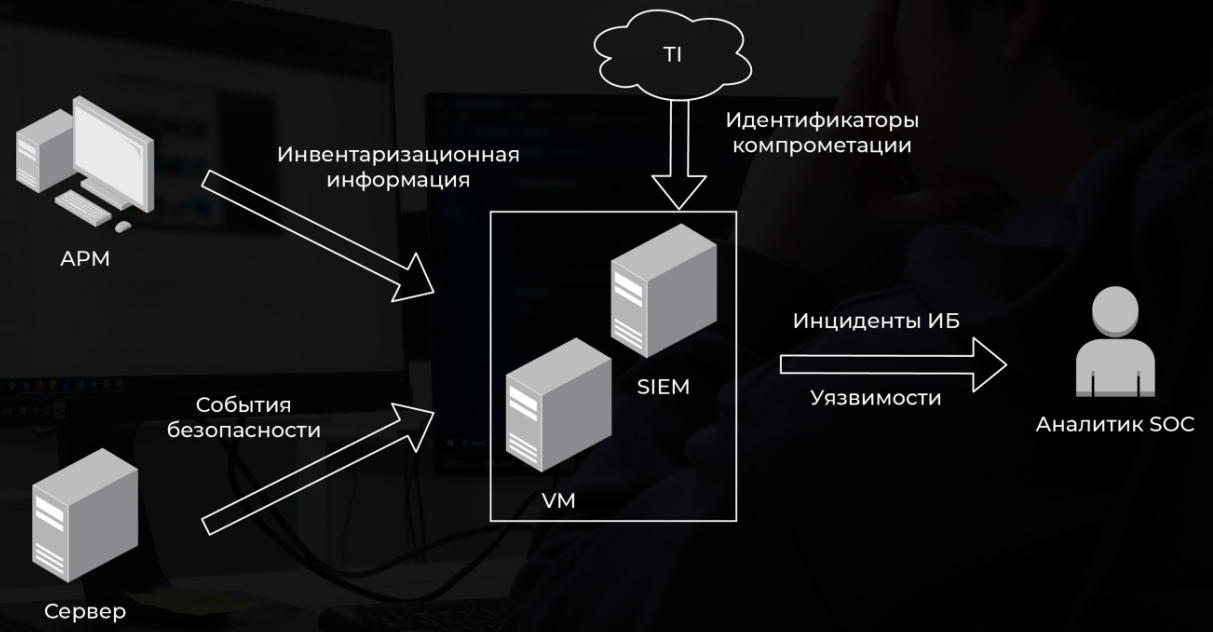


Как реализовано в SOCRAT?

Актуализация экспертизы SIEM за счет:

- Идентификаторов компрометации;
- Исключений по ложным инцидентам;
- Доработки правил на основе трендов угроз.

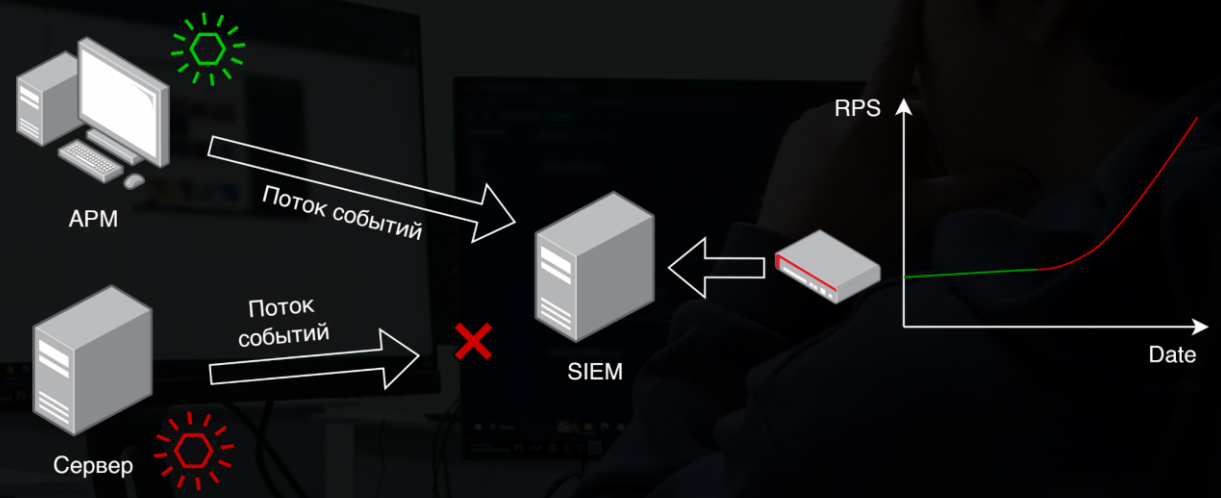
Интеграция SIEM с TI;
Интеграция SIEM с VM;
Предложения по расширению зоны мониторинга.



Инцидент может быть не только из-за атаки?

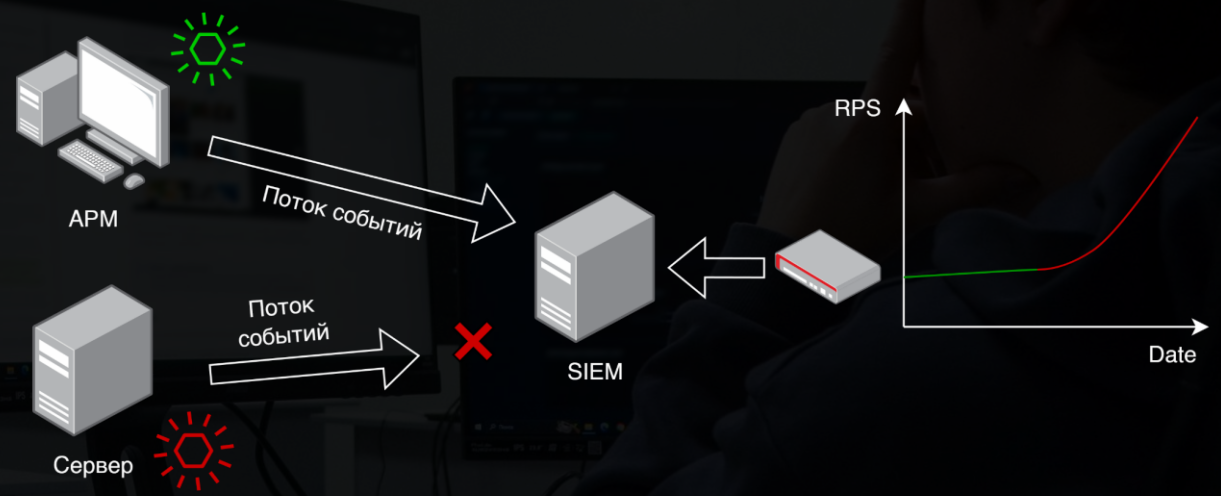
ГОСТ Р 59547-2021, раздел 4, п.4.2 в)
Анализ оценки функционирования систем защиты информации в ИС:

- Контроль работоспособности ПО и СЗИ;
- Проверка соответствия среды функционирования требованиям документации на СЗИ;
- Контроль потоков информации влияющих на производительность ИС;
- Информировать ответственного.



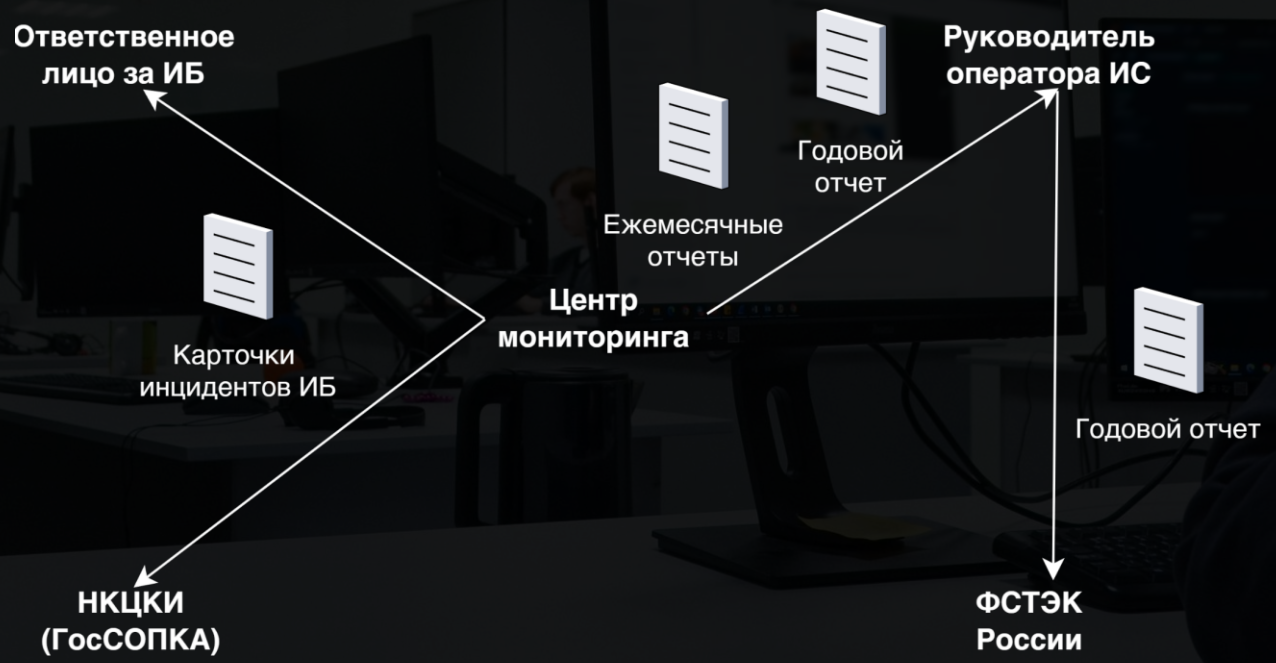
Как реализовано в SOCRAT?

- Контроль функционирования системы мониторинга и источников событий на основе потока событий;
- Контроль потока событий на наличие аномальных всплесков.



Кому сообщать об инцидентах ИБ?

Приказ № 117, раздел 3, пп.49
Приказ № 117, раздел 3, x)



Итоговый отчет отправляется руководителем оператора ИС во ФСТЭК России

Как реализовано в SOCRAT?

В случае обнаружения инцидента, либо подозрения на инцидент:

- Отправка карточки инцидента через АльфаИнциденты;
- Подготовка ежемесячных отчетов через АльфаИнциденты и отправка ответственному;
- Подготовка годового отчета и отправка ответственному;

В рамках пакета услуг производится взаимодействие с ГосСОПКА (интеграция АльфаИнциденты с ЛК ГосСОПКА)

Для самостоятельного взаимодействие, через АльфаИнциденты выгружается карточка в формате НКЦКИ для отправке на почту НКЦКИ

Выполняйте требования по мониторингу событий ИБ согласно 117 приказу ФСТЭК России за 1,9 млн.руб.

с командой SOCRAT

100

Анализ
до 100 активов

НПА

Мониторинг по ГОСТ Р
59547-2021 и 117
приказу ФСТЭК России

24/7

Непрерывный
мониторинг

A

Корпоративный
центр ГосСОПКА
(класс А)

SOC RAT
SECURITY OPERATION CENTER RUSSIAN ANALYTICS TEAM

SOCRAT – ЭТО ЦЕНТР МОНИТОРИНГА КСБ-СОФТ

Режим работы 24x7

Корпоративный центром ГосСОПКА (класс А)

Инвентаризация
Анализ Уязвимостей
Тестирование на проникновение

Пакетная система предоставления услуг (выбор только необходимого)

Год создания: 2020

С чего начать?

ПИЛОТНОЕ ПОДКЛЮЧЕНИЕ

Вы можете бесплатно оценить качество предоставляемых услуг **SOCRAT**

РАБОТАЙТЕ С НАМИ!

ksb-soft.ru

Телеграм-канал
«Мнение Интегратора»

Подкаст
«Голос Интегратора»

info@ksb-soft.ru

8 800 3333-872

428000, г. Чебоксары,
пр-т Максима Горького,
18 Б, пом. 9