КСБ-СОФТ

# 117 приказ ФСТЭК РФ: от «бумажной» безопасности к непрерывной и практической защите. Мониторинг – прогнозирование рисков


- **Илья Хохлов**
  Пресейл-инженер группы партнерского пресейла группы компаний «Солар»
- **Дмитрий Чирков**
  Руководитель регионального направления КСБ-СОФТ
- **Александр Кирий**
  Руководитель центра мониторинга SOCRAT

Длительность 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 3-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

**6000+**

реализованных проектов

SOCRAT
SECURITY OPERATION CENTER RUSSIAN ANALYTICS TEAM

# SOCRAT – ЭТО ЦЕНТР МОНИТОРИНГА КСБ-СОФТ

**Режим работы 24x7**

**Корпоративный центр ГосСОПКА**
(класс А)

- ✓ **Инвентаризация**
- ✓ **Анализ уязвимостей**
- ✓ **Тестирование на проникновение**

**Пакетная система предоставления услуг**
(выбор только необходимого)

**Год создания: 2020**

# О компании ГК «СОЛАР»

SOLAR

## ГК «СОЛАР» — ВЕДУЩИЙ ПОСТАВЩИК РЕШЕНИЙ КИБЕРБЕЗОПАСНОСТИ В РОССИИ

Обеспечивает киберзащиту крупных политических, экономических и социальных мероприятий, таких как:

- Выборы Президента РФ
- ПМЭФ
- «Игры Будущего»
- Всемирный фестиваль молодежи
- ФИФА-2018

### КЛЮЧЕВЫЕ НАПРАВЛЕНИЯ

Разработка собственных продуктов

Обучение ИБ-специалистов

Аутсорсинг ИБ

### ЦЕНТР ИССЛЕДОВАНИЯ КИБЕРУГРОЗ SOLAR 4RAYS

4RAYS by SOLAR

### ГК «СОЛАР» УЧАСТВУЕТ В РЕАЛИЗАЦИИ ВСЕРОССИЙСКОЙ ПРОГРАММЫ КИБЕРГИГИЕНЫ

Минцифры России

**10**
Лет на рынке ИБ

**200+** МЛРД
Анализируемых событий ИБ

**2500**
Экспертов по кибербезопасности

**1000+**
Организаций под защитой, включая более 70 из топ-100 российского бизнеса

# Приказ ФСТЭК №117

Вступил в силу с 1 марта 2026 года

**Запись вебинара 5 марта**

117 приказ ФСТЭК: от «бумажной» безопасности к непрерывной и практической защите. Новые реалии ИБ

SOLAR

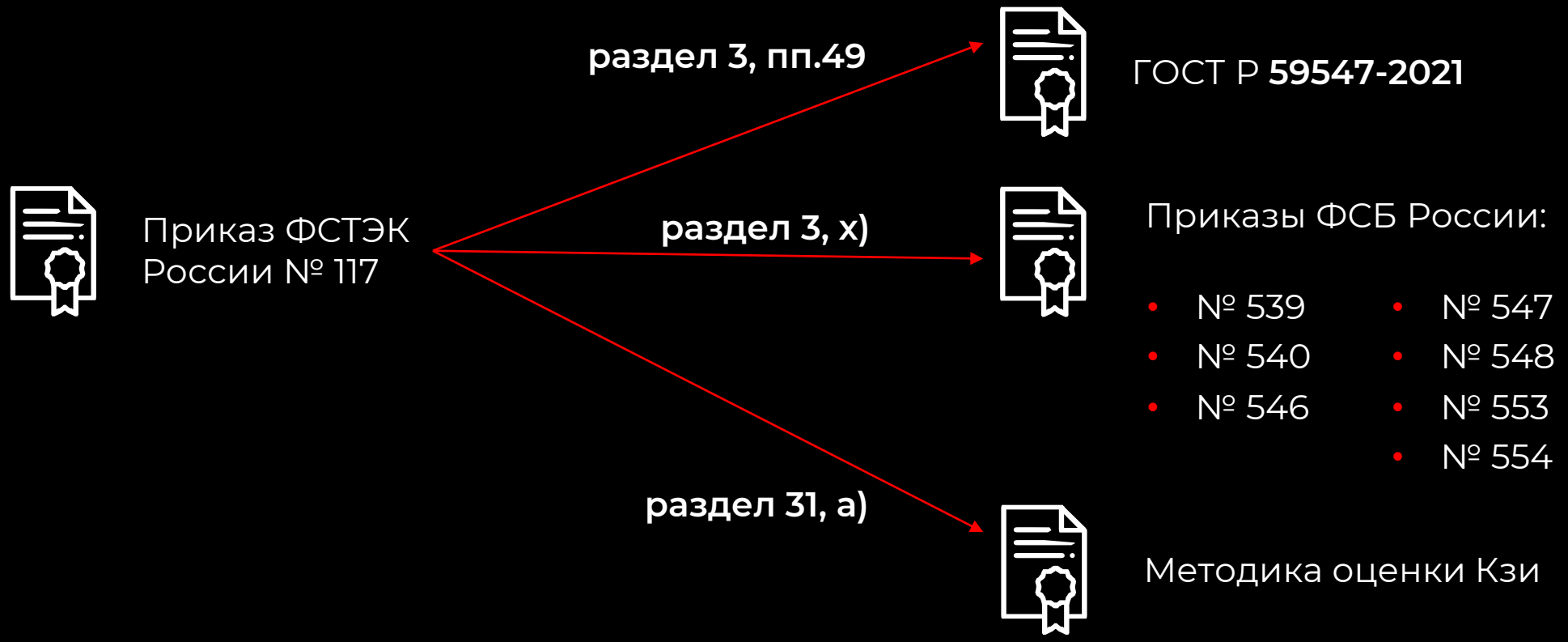
Требования распространяются на ГИС, иные информационные системы государственных органов, государственных унитарных предприятий и государственных учреждений

Отменяет Приказ ФСТЭК № 17

Аттестаты соответствия на ГИС и иные ИС, выданные до дня вступления в силу приказа ФСТЭК № 117, считаются действительными

Состав программных и программно-аппаратных средств определяется во внутренних стандартах и регламентах по защите информации

# Требования к мониторингу и ГосСОПКА в КИИ, ГИС и иных ИС ОГВ



# Состав мероприятий

## Сбор событий ИБ и их анализ

- Приказ № 117, раздел 3, пп.49
- ГОСТ Р 59547-2021, раздел 4, п.4.1, 4.2 а)
- Методика оценки Кзи, таблица 1, группа №4, 1–2 показатели

## Анализ защищенности

- Приказ № 117, раздел 3, пп.38
- ГОСТ Р 59547-2021, раздел 4, п.4.2 б)

## Анализ систем защиты информации

- ГОСТ Р 59547-2021, раздел 4, п.4.2 в)

## Анализ изменения угроз безопасности

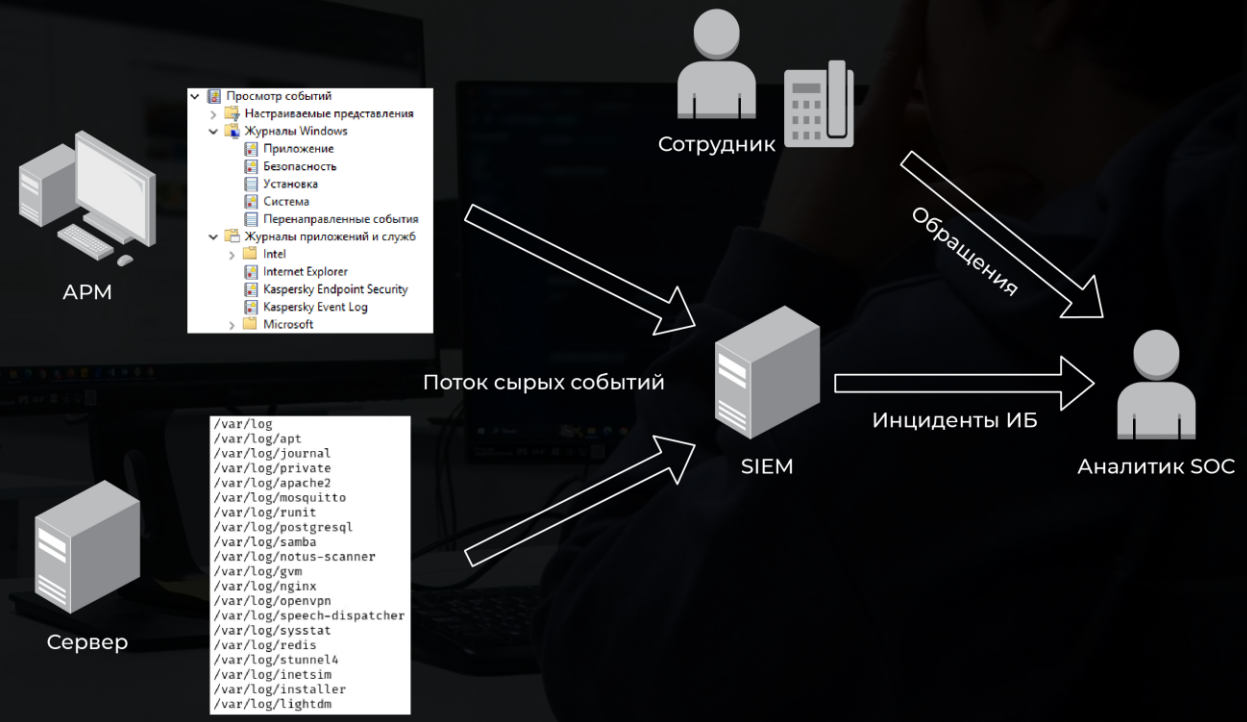
- ГОСТ Р 59547-2021, раздел 4, п.4.2 г)

## Взаимодействие с ГосСОПКА

- Приказ № 117, раздел 3, х)
- Приказы ФСБ России

# Сбор событий ИБ и их анализ. Технологии

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



SOLAR

## ЭКСПЕРТИЗА В ПОСТРОЕНИИ ЦЕНТРОВ SOC

Знания о реальных болях и задачах, решаемых в инфраструктуре крупных заказчиков

# Solar SIEM

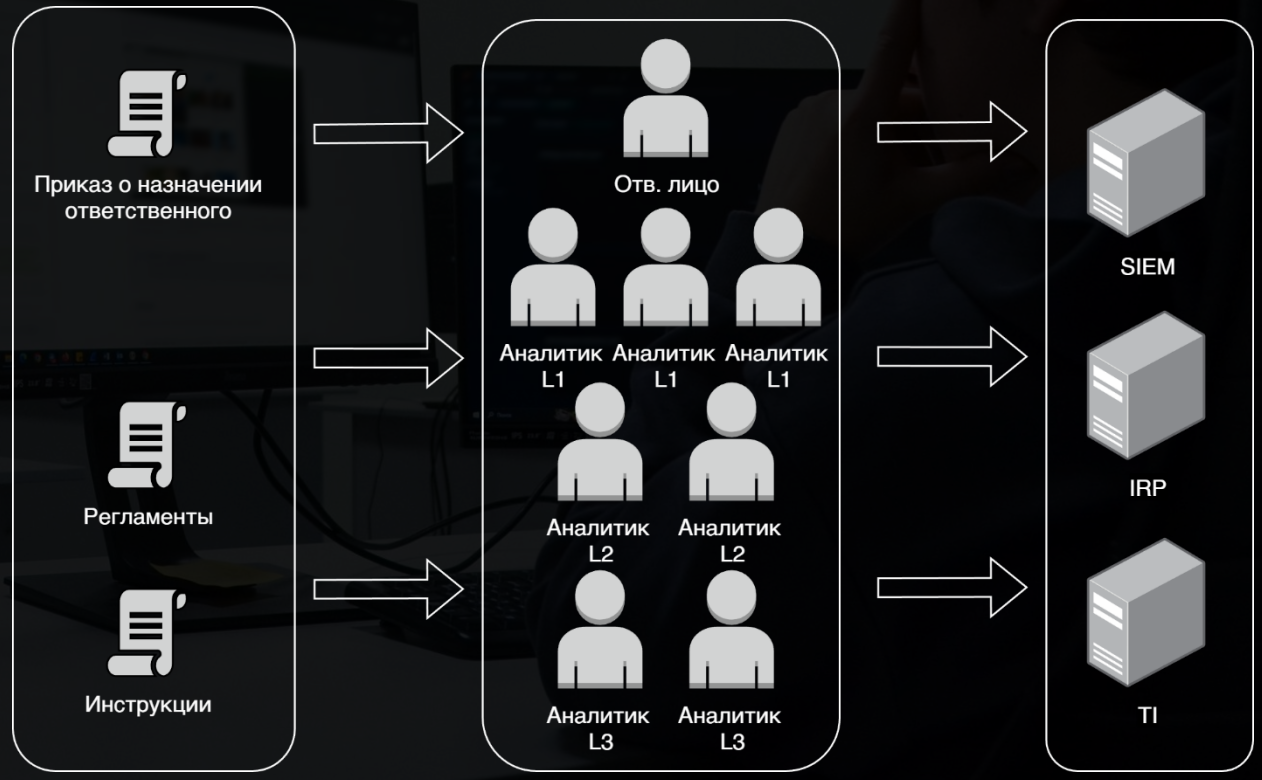
SOLAR

Новый автоматизированный программный комплекс, который объединяет функциональность SIEM и SOAR в едином решении и обеспечивает:

- Централизованный сбор и обработку событий ИБ в режиме реального времени
- Интеллектуальное выявление угроз
- Автоматизацию процессов реагирования на инциденты ИБ

# Сбор событий ИБ и их анализ. Люди и процессы

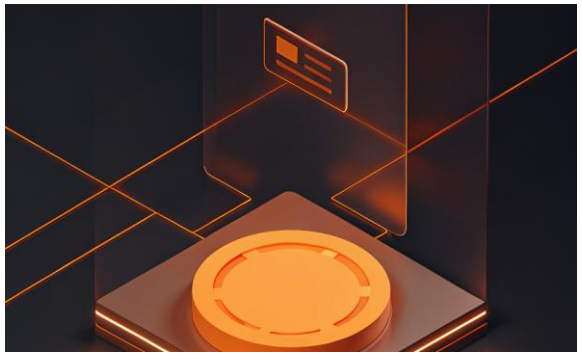
- Определение состава контролируемых ресурсов
- Разработка инструкций, сценариев реагирования, регламентов
- Организация взаимодействия с НКЦКИ (ГосСОПКА)
- Контроль за исполнением



# Solar SIEM — единый инструмент полного цикла защиты: от мониторинга до реагирования

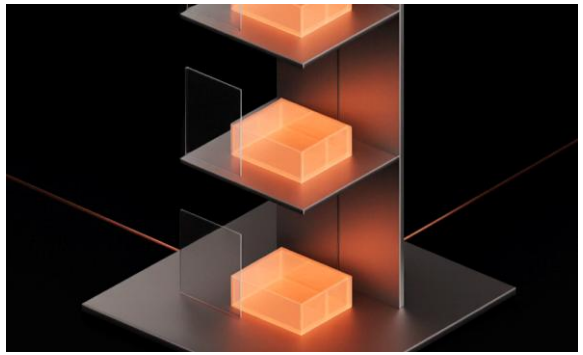
Внесен в РОПО:
№ 21682 от 07.03.2024

Сертификат ФСТЭК России
СОВ.У4: Q2 2026



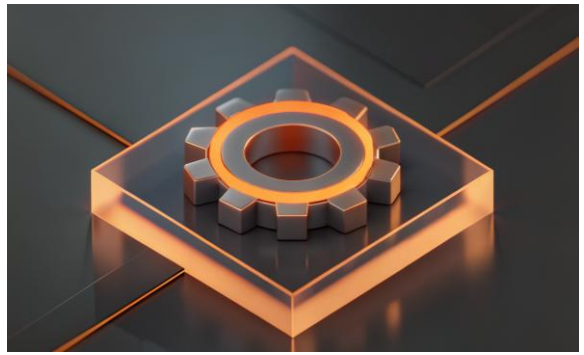
## ОБЪЕДИНЕНИЕ SIEM И SOAR В ОДНОМ РЕШЕНИИ

Позволяет оптимизировать бюджет и снизить сложность интеграции



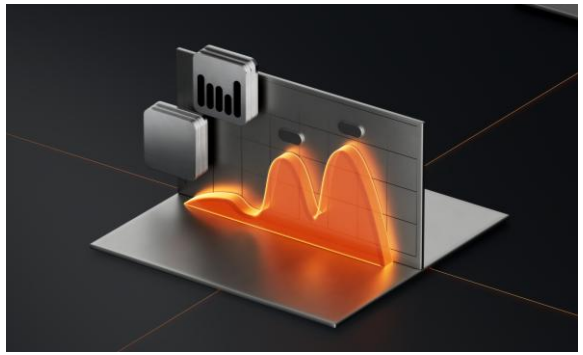
## ВСТРОЕННЫЕ СЦЕНАРИИ РЕАГИРОВАНИЯ

Сокращает Time-to-Response и автоматизирует процесс реагирования



## ПРОФИЛИРОВАНИЕ ДАННЫХ

Автоматизирует агрегацию данных и ускоряет расследование



## AI-ПОМОЩНИК

Снижает порог вхождения специалистов первой линии и визуализирует процесс реагирования

# Защита информации при использовании конечных устройств

SOLAR

EDR

Программный продукт/сервис для защиты от кибератак, устанавливается на рабочие станции и серверы. Мониторит активность, собирает телеметрию, выявляет APT-угрозы, блокирует вредоносные действия и помогает расследовать инциденты

## КАКИЕ ТРЕБОВАНИЯ ЗАКРЫВАЕТ

П.41 – исключение возможности несанкционированного доступа к информационным системам и конечным устройствам или воздействия на них через интерфейсы и порты, непосредственно взаимодействующие с сетью Интернет и (или) доступные из сети Интернет

## ПРЕИМУЩЕСТВА ПРОГРАММНОГО ПРОДУКТА

- модули сбора событий на уровне kernel- и user-space
- возможность собирать любые события на узле (11 категорий, 80 типов событий)
- 2-уровневая префильтрация при сборе данных для анализа именно тех событий, которые имеют наибольшее значение для конкретной инфраструктуры
- правила детектирования от Solar 4RAYS
- самозащита системы: независимость от встроенного функционала ОС и скрытность от пользователя
- использование драйверных модулей, минимизирующих возможность подмены события

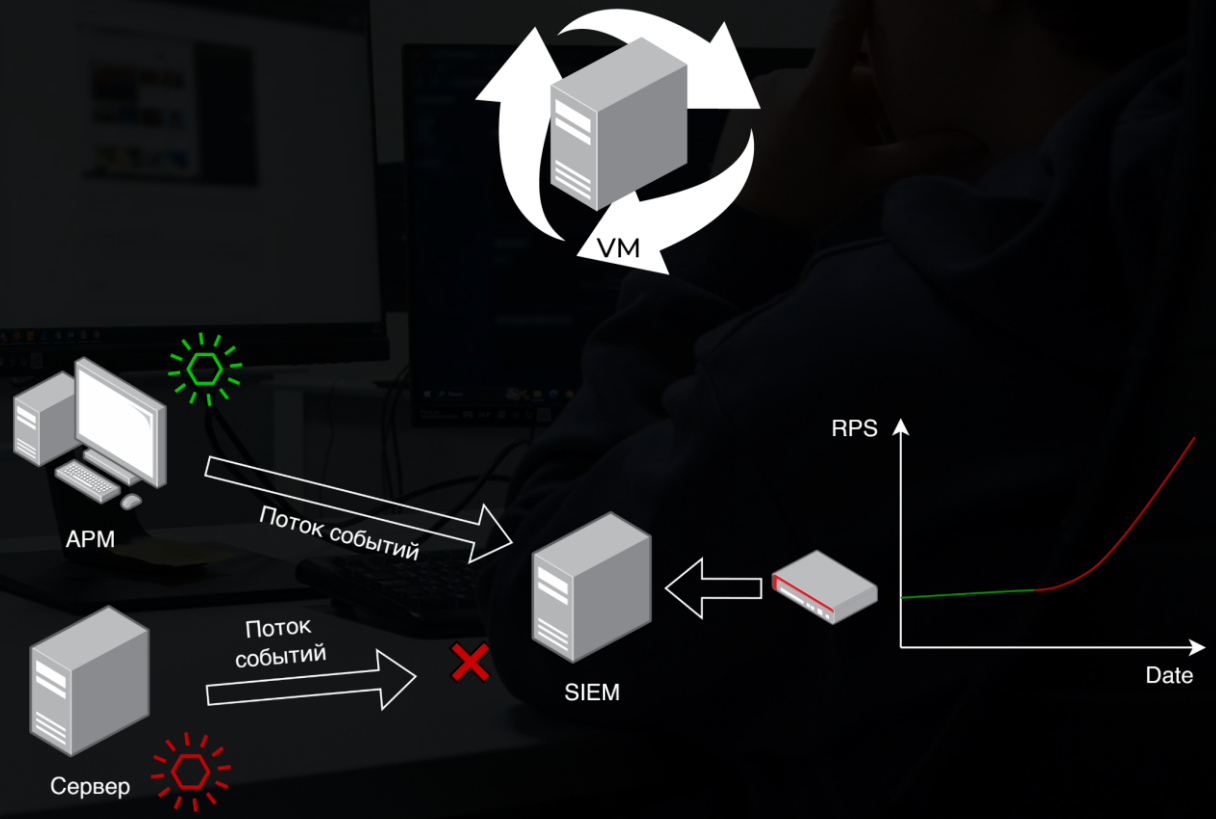
Собственный легковесный агент на Windows и Linux

Внесен в РОПО:
№ 24710 от 15.11.2024

# Анализ защищенности и анализ систем защиты информации

- Выявлять уязвимости
- Контролировать установку обновлений
- Проводить инвентаризацию
- Контролировать настройку ПО и СЗИ в соответствии с политиками ИБ

- Контроль работоспособности ПО и СЗИ
- Контроль потоков информации, влияющих на производительность ИС



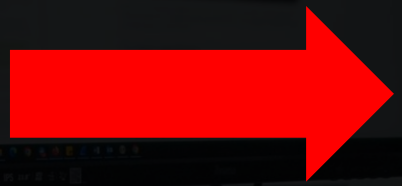
# Анализ защищенности и анализ систем защиты информации

**ИТ-процессы**

- Периодическая инвентаризация (актуализация и учет активов сети)
- Обновление версий ПО и ОС (особенно установка пакетов безопасности)
- Контроль работоспособности систем

**ИБ-процессы**

- Выявление и описание уязвимостей
- Контроль установки и настройки средств защиты



**Снижение вероятности инцидента**

# Контроль конфигураций ИС

SOLAR

Solar Lighthouse

позволяет эффективно интегрироваться с различными источниками информации, проводить активные сканирования инфраструктуры, реализовывать аудит соответствия требованиям и строить процессы по обеспечению безопасности инфраструктуры

## КАКИЕ ТРЕБОВАНИЯ ЗАКРЫВАЕТ

П.37 – исключение несанкционированного изменения состава программных, программно-аппаратных средств информационных систем, их настроек и конфигураций, установленных во внутренних стандартах по защите информации, обеспечение обнаружения фактов несанкционированных изменений и выявление причин изменений. Контроль должен осуществляться на основе анализа результатов учета ИТ-активов и (или) сведений, содержащихся в автоматизированных системах хранения и управления данными об информационных системах и их конфигурациях

## ПРЕИМУЩЕСТВА

- эталонные конфигурации (baseline) для классов систем и ролей (серверы, рабочие станции, периметр, удалённый доступ и т.п.)
- выявление отклонений: что именно изменилось, когда, на каких узлах, чем это опасно
- интеграция с инвентаризацией/CMDB (или сам выступает источником актуальных данных об активах)
- формирование базы: какие настройки были, какие стали, как вернуть к стандарту
- включен в Реестр отечественного ПО

## ТАКЖЕ ЗАКРЫВАЕТ:

- ✓ ТРЕБОВАНИЯ ПО УПРАВЛЕНИЮ ОБНОВЛЕНИЯМИ (П.39)
- ✓ ЧАСТЬ ТРЕБОВАНИЙ ПО УПРАВЛЕНИЮ УЯЗВИМОСТЯМИ (П.38)

# Примеры решаемых задач с LightHouse

## Знания об инфраструктуре

- Сбор перечня ассетов со всех возможных систем
- Выявление новых ассетов в инфраструктуре
- Определение владельцев для всех ассетов в инфраструктуре
- Определение критичности ассетов
- Определение вхождения ассета в ИТ системы

## Практики безопасности

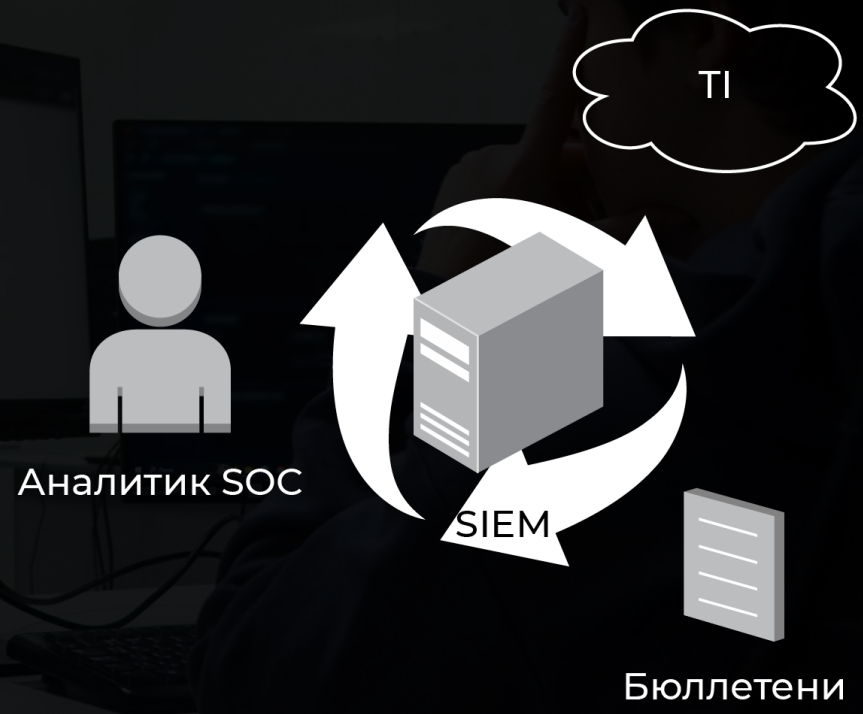
- Контроль установленного ПО согласно белому/черному списку
- Запуск и контроль корректности работы патч-менеджмента
- Контроль параметров и версий СЗИ
- Проверка корректности сетевой сегментации
- Обеспечение «чистого» периметра

## Смежные задачи

- Контроль сроков действий лицензий
- Менеджер задач для упрощения взаимодействия
- Оценка соответствия по реальному состоянии инфраструктуры и процессов
- Переводчик с ИБшного
- Учёт и экономия используемых ИТ ресурсов

# Анализ изменения угроз безопасности

- Анализ изменения угроз: открытые источники, TI-платформы
- Бюллетени регуляторов (ФСТЭК, НКЦКИ)
- Анализ собранных событий безопасности



# Solar TI Feeds это:

## ДАННЫЕ ОБ АКТУАЛЬНЫХ КИБЕРУГРОЗАХ В РФ ИЗ УНИКАЛЬНЫХ ИСТОЧНИКОВ

- Сведения от сенсоров в сети крупнейшего телеком-оператора «Ростелеком»
- Телеметрия сервисов крупнейшего центра противодействия Solar JSOC и топ-5 в рейтинге MSSP Европы
- Результаты собственной киберразведки и более 200 расследований Solar 4RAYS

## ЗНАНИЯ О ВРЕДОНОСНЫХ КАМПАНИЯХ 24/7

Ежедневно фиксируются и обрабатываются:

- 200+ млрд событий на сенсорах
- 3+ млн алертов
- 1+ млн действий хакеров

После автоматической и ручной проверки остаются только сведения о самых опасных и актуальных угрозах:

- ИНДИКАТОРЫ КОМПРОМЕТАЦИИ
  IP-адреса, домены, веб-ссылки, хеш-суммы
- ИНДИКАТОРЫ АТАК
  Правила обнаружения Suricata, YARA, Sigma, ModSec

## ПРОВЕРЕННЫЕ ЗНАНИЯ БЕЗ ФОЛЗОВ

- Проверяем и обкатываем правила на крупнейшем коммерческом SOC в РФ
- Подтверждаем полезность фидов при проведении собственных расследований
- Даем возможность оценить качество данных на пилотном подключении

# Возможности и состав Solar Threat Intelligence

## SOLAR TI FEEDS

Непрерывное усиление SOC
с помощью уникальных фидов
для раннего обнаружения
и реагирования на угрозы

Solar TI Feeds позволяет подключать только необходимый состав потоков данных под ваши текущие задачи, с возможностью дальнейшего апгрейда и масштабирования

СОСТАВ СЕРВИСА

### ПОТОКИ ДАННЫХ (ФИДЫ)

**IOC**
Индикаторы компрометации

**IOA**
Индикаторы атак

| КАТЕГОРИИ ДАННЫХ |
|---|
| APT |
| CYBERCRIME |
| PHISHING |
| ACTIVE_C2 |
| HONEYPOT |
| INTRUSION |
| FINCERT |
| VPN |
| PROXY |
| TOR |
| Сигнатуры IDS |
| Сигнатуры IDS_TREND |
| Правила WAF |
| Правила YARA_WINDOWS |
| Правила YARA_LINUX |
| Правила YARA_TREND_WINDOWS |
| Правила YARA_TREND_LINUX |
| Правила SIGMA_WINDOWS |
| Правила SIGMA_LINUX |
| Правила SIGMA_TREND_WINDOWS |
| Правила SIGMA_TREND_LINUX |
| Правила SIGMA_KUBERNETES |

### КАСТОМИЗАЦИЯ ФИДОВ

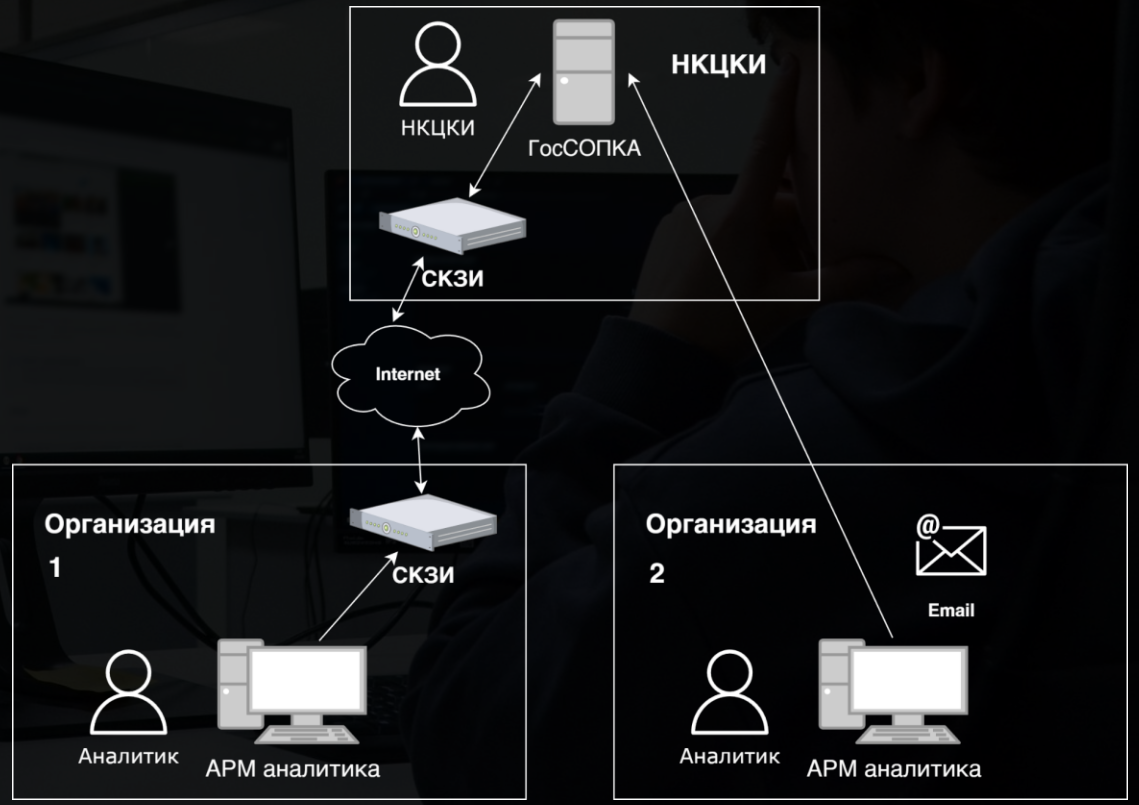
- Поставка более 20 готовых фидов
- Готовые 4 комплекта под ключевые задачи служб ИБ
- Индивидуальная настройка фильтров, срезов и правил

### ИНТЕГРАЦИЯ С СЗИ

- SIEM-, SOAR-системы, NGFW, EDR, XDR и т. п.
- TI-платформы

# Взаимодействие с ГосСОПКА

- Уведомлять в случае обнаружения КА и КИ в течение 24 часов (ЗОКИИ – 3 часа)
- При наличии взаимодействия с ТИ НКЦКИ, отправлять уведомления через личный кабинет (обязательно для ЗОКИИ)
- При отсутствии взаимодействия с ТИ НКЦКИ – по адресам НКЦКИ



# Реализация мер по защите ИС и содержащейся в них информации. Базовые меры защиты (п.63)

SOLAR

УПРАВЛЕНИЕ ДОСТУПОМ

ЗАЩИТА ТЕХНОЛОГИЙ КОНТЕЙНЕРНЫХ СРЕД И ИХ ОРКЕСТРАЦИИ

ЗАЩИТА ЭЛЕКТРОННОЙ ПОЧТЫ

ЗАЩИТА ВЕБ-ТЕХНОЛОГИЙ

РЕГИСТРАЦИЯ СОБЫТИЙ БЕЗОПАСНОСТИ

# ЧТО ЕЩЕ ВХОДИТ В 117 ПРИКАЗ ФСТЭК РФ

SOLAR

УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ (П.38)

УПРАВЛЕНИЕ ОБНОВЛЕНИЯМИ (П.39)

ЗАЩИТА ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА ПРИ ЕЁ ОБРАБОТКЕ, ХРАНЕНИИ И ОБРАЩЕНИИ (П.40)

ЗАЩИТА ИНФОРМАЦИИ ПРИ ПРИМЕНЕНИИ МОБИЛЬНЫХ УСТРОЙСТВ И УДАЛЕННОМ ДОСТУПЕ ПОЛЬЗОВАТЕЛЕЙ (П.42, 45, 46)

ЗАЩИТА ПРИВИЛЕГИРОВАННОГО ДОСТУПА И ВЗАИМОДЕЙСТВИЕ С ПОДРЯДНЫМИ ОРГАНИЗАЦИЯМИ (П.48, 58)

РАЗРАБОТКА БЕЗОПАСНОГО ПО (П.50)

ПОВЫШЕНИЕ УРОВНЯ ЗНАНИЙ И ИНФОРМИРОВАННОСТИ ПОЛЬЗОВАТЕЛЕЙ ИС В ВОПРОСАХ ЗАЩИТЫ ИНФОРМАЦИИ (П.56)

ЗАЩИТА ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ ИСКУСТВЕННОГО ИНТЕЛЛЕКТА (П.60)

КОНТРОЛЬ УРОВНЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ (П.66)

# С чего начать?

**ПИЛОТНОЕ ПОДКЛЮЧЕНИЕ к 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**

# РАБОТАЙТЕ С НАМИ!

ksb-soft.ru

**Канал в MAX**
«Мнение Интегратора»

**Подкаст**
«Голос Интегратора»

info@ksb-soft.ru

8 800 3333-872

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