SOLAR

Solar SIEM

ПРОГРАММНЫЙ КОМПЛЕКС АВТОМАТИЗАЦИИ
СИТУАЦИОННОГО ЦЕНТРА ИБ

2025

Объединение усилий «Солар» + «Гефест»

SOLAR

ЭКСПЕРТИЗА В ПОСТРОЕНИИ ЦЕНТРОВ SOC

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

heftech

ОПЫТ РАЗРАБОТКИ МИРОВОГО УРОВНЯ

Опыт создания решений для Microsoft, Dell, HP и других компаний из Fortune 500

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

Актуальность задач мониторинга и реагирования

SOLAR

~2500

Инцидентов происходит в крупных организациях в течение года

~80%

Инцидентов остаются незамеченными без централизованной системы корреляции и реагирования

ВЫЗОВЫ ДЛЯ БИЗНЕСА

ДЕФИЦИТ КАДРОВ

Компетентных специалистов по ИБ мало, их обучение стоит дорого, а удержать кадры — трудно

ТРЕБОВАНИЯ РЕГУЛЯТОРОВ

Указы Президента РФ № 250 и 166, 187-ФЗ, рекомендации НКЦКИ

ОГРАНИЧЕНИЕ БЮДЖЕТОВ НА ИБ

Рост стоимости ИБ-решений происходит на фоне ограничения финансирования ИБ

СОКРАЩЕНИЕ TIME-TO-ATTACK

Автоматизация и ИИ используются не только защитниками, но и злоумышленниками

СЛОЖНОСТЬ И НИЗКАЯ АДАПТИВНОСТЬ SIEM-СИСТЕМ

Классические SIEM сложны во внедрении, подключение источников, контроль полноты и качества логов — трудозатратны и непрозрачны

РАЗРОЗНЕННОСТЬ ИНСТРУМЕНТОВ

Использование раздельных продуктов (SIEM, SOAR, EDR, VM) увеличивает стоимость защиты и создает «слепые зоны» на стыке систем и лицензий

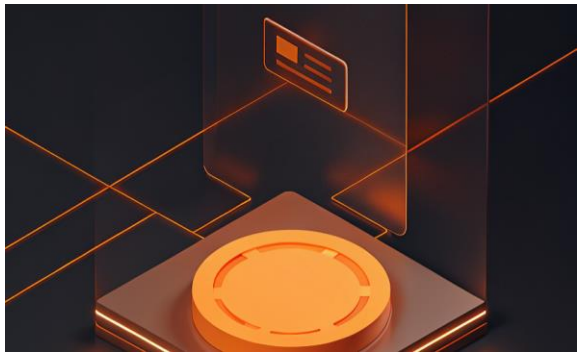
Источники: исследование ГК «Солар», 2025

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

SOLAR

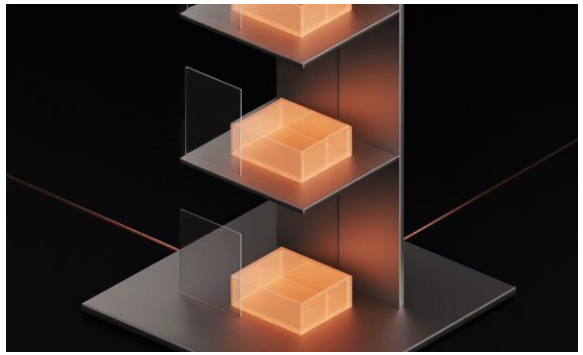
Внесен в РОПО:
№ 21682 от 07.03.2024

Сертификат ФСТЭК России
СОВ.У4: Q1 2026



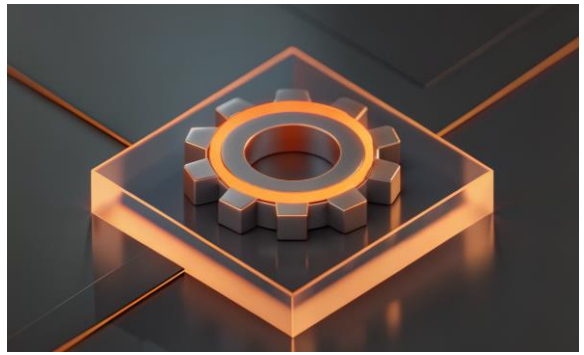
ОБЪЕДИНЕНИЕ SIEM И SOAR В ОДНОМ РЕШЕНИИ

Позволяет оптимизировать бюджет и снизить сложность интеграции



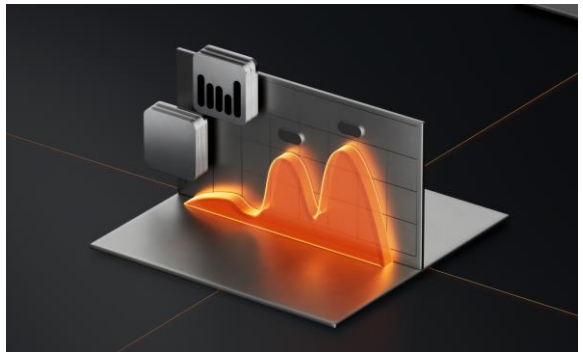
ВСТРОЕННЫЕ СЦЕНАРИИ РЕАГИРОВАНИЯ

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

Ключевые возможности Solar SIEM

01

МОНИТОРИНГ И КОРРЕЛЯЦИЯ СОБЫТИЙ

Сбор событий из множества источников, функционирующих на устройствах Linux и Windows, включая, но не ограничиваясь:

- Системные журналы (Linux Syslog, Windows Event Log)
- Базы данных (PostgreSQL, Oracle, MySQL, Microsoft SQL Server)
- Файлы журналов СЗИ и ПО (Microsoft Windows Defender Firewall, Microsoft DHCP Server, Microsoft Windows DNS Server, Microsoft IIS Server, Microsoft Network Policy Server)
- Журналы формата CEF
- Файлы журналов произвольного формата

Нормализация и обогащение собранных событий на основе создаваемых пользователями правил, а также настройка правил

Передача данных исходных и обогащенных событий в хранилище программного комплекса для дальнейшей обработки и анализа

SOLAR

Ключевые возможности Solar SIEM

02

СБОР, ОБРАБОТКА И ХРАНЕНИЕ СОБЫТИЙ

Анализ исходных, нормализованных и обогащенных событий на наличие угроз ИБ в автоматическом и ручном режимах

03

УПРАВЛЕНИЕ И ВЫПОЛНЕНИЕ СЦЕНАРИЕВ РЕАГИРОВАНИЯ

Создание и настройка сценариев для автоматизации и ускорения реагирования на события и инциденты ИБ, повышения эффективности их обработки.

Пошаговое выполнение сценариев реагирования в автоматическом и полуавтоматическом режимах

SOLAR

Ключевые возможности Solar SIEM

04

УПРАВЛЕНИЕ СОБЫТИЯМИ И ИНЦИДЕНТАМИ ИБ

Формирование карточки событий и инцидентов ИБ для фиксации связанной с ними информации.

Возможность связывания правил корреляции с созданными сценариями реагирования.

Централизованное управление логикой генерации алертов и инцидентов

05

ВИЗУАЛИЗАЦИЯ МЕТРИК ИБ

Графическое представление операционных, статистических и аналитических данных о работе ситуационного центра

06

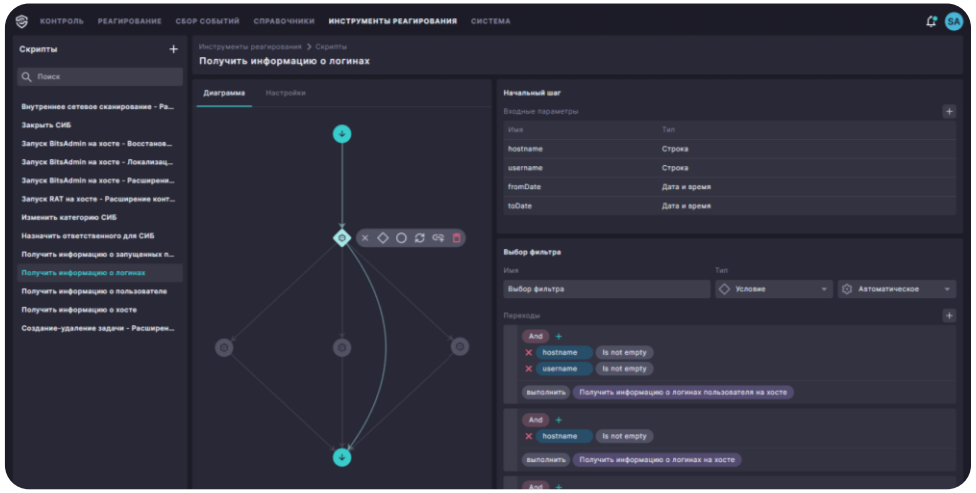
ФОРМИРОВАНИЕ ОТЧЕТНОСТИ

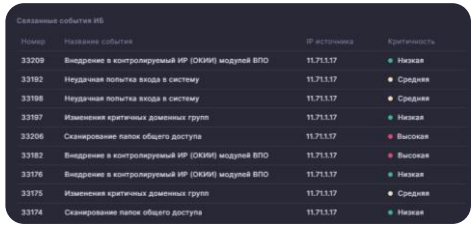
Сохранение зарегистрированных событий и инцидентов ИБ в формате CSV.

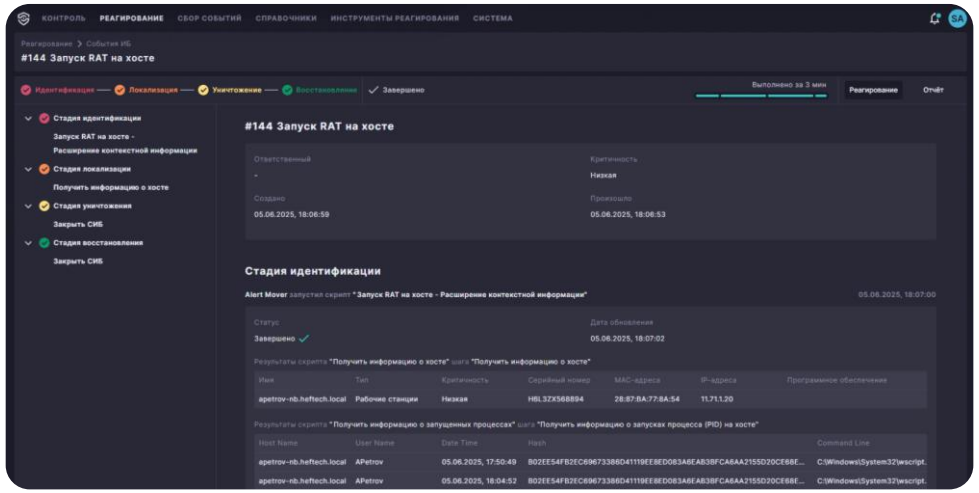
Поддержка экспорта отчетов в форматах XLSX и PDF

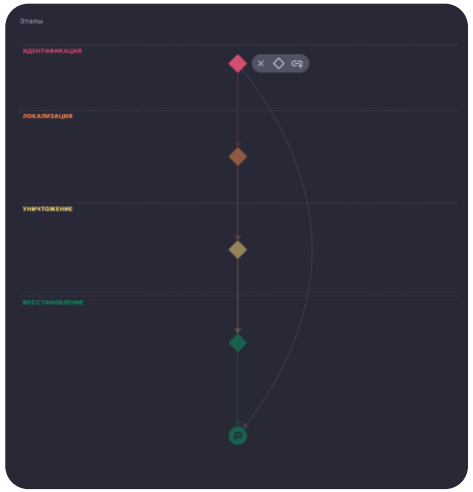
Веб-интерфейс Solar SIEM

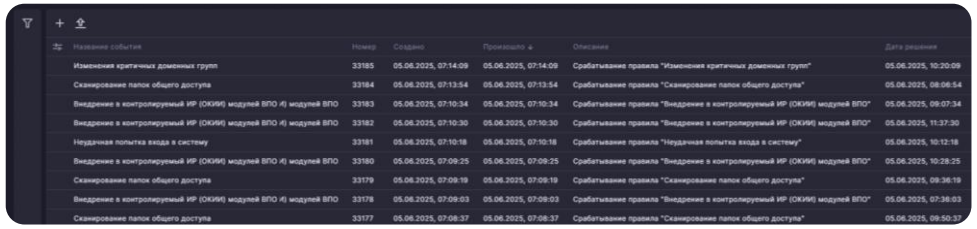
Управление Solar SIEM осуществляется через единую консоль, доступную из веб-браузера. Ее интерфейс спроектирован по принципу ситуационного центра и позволяет службе безопасности оперативно оценить обстановку, выделить приоритетные направления работы и начать обработку событий и реагирование на инциденты





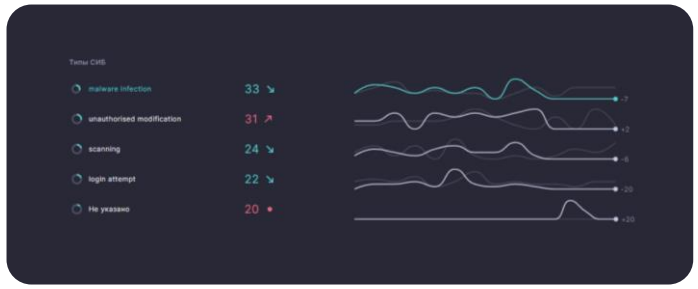


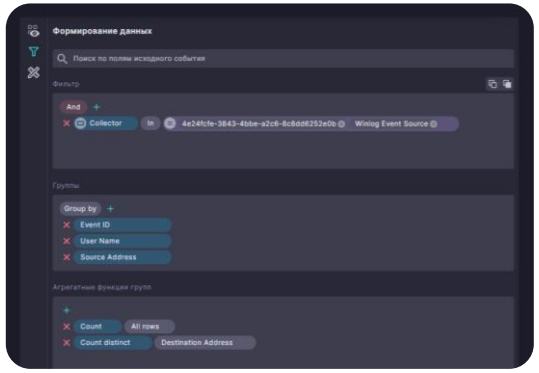


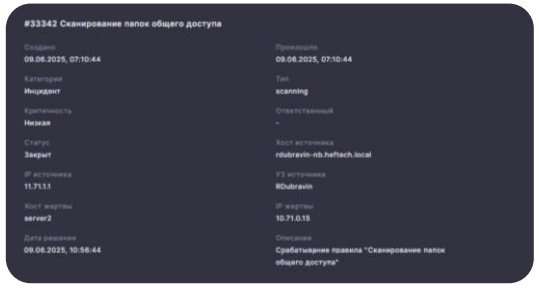


Веб-интерфейс Solar SIEM

Для работы с Solar SIEM не требуется глубоких технических знаний. Унифицированный подход к UI/UX через использование визуального языка позволяет интуитивно управлять сложными процессами и сокращает время на обучение новых пользователей







В чем уникальность Solar SIEM

SOLAR

АВТОМАТИЗАЦИЯ

АНАЛИТИКИ И ОБРАБОТКИ ДАННЫХ

Автоматический сбор расширенного контекста сработанного правила корреляции на основе полученных данных (системные журналы Windows и Linux, БД, СЗИ, внешние системы)

ОБНОВЛЕНИЯ КОНТЕНТА

Непрерывная доставка новых правил корреляции, типов источников и парсеров логов в потоковом режиме

РЕАГИРОВАНИЯ

Встроенный модуль ручного или автоматизированного реагирования на выбор

ПРОФИЛИРОВАНИЕ ДАННЫХ

Оптимизация обращений к ретроспективным данным и создание своих профилей для сокращения времени анализа и реагирования

КОНСТРУКТОР СЦЕНАРИЕВ РЕАГИРОВАНИЯ В UI

Гибкая настройка сценариев реагирования: автоматизированное нативное обогащение, отправка запросов во внешние системы

КРАТНОЕ СЖАТИЕ ДАННЫХ ПРИ ХРАНЕНИИ

Коэффициент сжатия от 9,8 до 16,6

AI-ассистент: что умеет

ПОМОГАЕТ СОЗДАВАТЬ

- Правила корреляции событий
- Аналитические запросы к данным
- Сценарии автоматизированного реагирования

ПОНИМАЕТ

Обычный разговорный язык — достаточно просто сформулировать задачу

СОДЕЙСТВУЕТ ПРИ РАБОТЕ С ИНЦИДЕНТАМИ

- Подсказывает, какие запросы и почему нужно выполнить
- Сам формирует нужные команды и отправляет на исполнение
- Использует весь контекст инцидента: события, логи, предыдущие кейсы, MITRE-техники и др.

SOLAR

ЭКОНОМИТ ВРЕМЯ

ПОВЫШАЕТ ТОЧНОСТЬ

СНИЖАЕТ НАГРУЗКУ НА АНАЛИТИКОВ

Solar SIEM vs. Классический SIEM

SOLAR

КРИТЕРИЙ	ФУНКЦИЯ	SOLAR SIEM	КЛАССИЧЕСКИЙ SIEM
Работа с контентом	• Единый набор корреляционных правил для всех поддерживаемых источников событий • Конфигурация корреляционных правил без необходимости изменения кода правила • Настройка исключений по запущенным корреляционным правилам без необходимости изменения кода правила • Настройка сбора профилей данных	Доступно по умолчанию	Функциональность отсутствует
Хранение данных	• Кратное сжатие данных	Коэффициент сжатия — от 9,8 до 16,6	Коэффициент сжатия — от 0,5 до 1,3
Реагирование	• Запуск сценариев реагирования по расписанию • Визуализация шагов отработки сценария реагирования • Выполнение сценариев реагирования по запросу пользователя • Задание условия применения сценариев реагирования в зависимости от контекста реагирования • Выполнение шагов сценариев реагирования вручную • Выполнение шагов сценариев реагирования в автоматическом режиме	Доступно по умолчанию	Функциональность отсутствует
Автоматическое реагирование	• Автоматическое реагирование в результате срабатывания правила корреляции собственными средствами, сторонними средствами и через пользовательские скрипты	Доступно по умолчанию	Функциональность отсутствует либо через интегрированные решения

Solar SIEM vs. Зарубежные SIEM

SOLAR

КРИТЕРИЙ	SOLAR SIEM	SPLUNK, IBM QRADAR, MICRO FOCUS ARCSIGHT, FORTISIEM, RSA NETWITNESS, MCAFEE ESM
Поддержка и развитие в России Развитие в соответствии с требованиями регуляторов (187-ФЗ, НКЦКИ, ГосСОПКА)	✓	✗
Отсутствие санкционных рисков и гарантия доступности Прозрачный процесс обновлений и локальной технической поддержки	✓	✗
Экономическая эффективность • Отсутствие валютных контрактов • Выгодная лицензионная политика (SIEM+SOAR) • Сокращение TCO	✓	✗
Продукт, адаптированный под российскую инфраструктуру Учет особенностей ИТ-архитектуры российских компаний, включая интеграцию с отечественными СЗИ	✓	✗
Быстрое внедрение и сопровождение Преднастроенные правила и адаптированный контент от Solar JSOC	✓	✗

Развитие Solar SIEM в 2026 году

SOLAR

Март

SOLAR SIEM V2026.1

- Мультитенантность: единая cloud-инсталляция для нескольких бизнес-единиц
- AI-ассистент, который сам запускает команды интеграции
- AI-агент на потоке событий, собирающий контекст по kill chain
- Интеграция с TI FEEDS 4RAYS, расширение правил TH и раннего обнаружения IOC

Укрепление технологического ядра и регуляторной готовности, улучшенный корреляционный движок, получение сертификата ФСТЭК России

Solar SIEM готов к крупным и строго регулируемым внедрениям

Июнь

SOLAR SIEM V2026.2

- Мультитенантность: hybrid-сценарий с выносным коррелятором
- Второе мнение. AI-ассистент начинает активно анализировать события и строить kill chain
- AI-ассистент в работает в режиме диалога
- Интеграция с DNS Radar

Повышение продуктивности аналитиков и управление данными: «Второе мнение» становится рабочим инструментом, улучшается фильтрация событий

Оптимальный по бюджету продукт для распределенных инфраструктур

Сентябрь

SOLAR SIEM V2026.3

- Мультитенантность: hybrid-сценарий с централизованным управлением несколькими инсталляциями в одном окне
- Расширенная двусторонняя интеграция со сторонними SOAR / IRP
- Прототип модуля анализа аномалий
- Интеграция с EDR

Фокус на управлении сложными инфраструктурами и доработка модуля реагирования. Релиз помогает строить промышленный SOC для групп компаний, защищать от сложных APT-атак

Декабрь

SOLAR SIEM V2026.4

- Мультитенантность: cloud-сценарий с авто-подстройкой ресурсов (подход Pay-as-you-go) и управлением всеми параметрами из UI
- Релиз модуля анализа аномалий

Перевод Solar SIEM в режим проактивной, экономически гибкой платформы для долгосрочной защиты

Подходит для использования по модели MSSP

Поставляемая экспертиза

SOLAR

	Q2 2025	Q3 2025	Q4 2025	Q1 2026	Q2 2026	Q3 2026
Правила THREAT HUNTING	50	200	300	350	400	450
Сценарии SOLAR JSOC	-	40	60	90	120	150
Поддерживаемые источники	15	34	48	69	91	112
Поведенческие профили	-	-	15	15	15	15

Как лицензируется Solar SIEM

SOLAR

МЕТРИКИ ЛИЦЕНЗИРОВАНИЯ

- Количество EPS в диапазоне от 250 до 499 999

- Уровень предоставляемой поддержки (SLA):
  - «Стандарт»
  - «Премиум» *

- Дополнительные возможности:
  - Повышенная доступность
  - Поддержка ГосСОПКА
  - Поддержка ГосСОПКА. Повышенная доступность

КОМПЛЕКТАЦИЯ

Solar SIEM лицензируется в виде программного комплекса в составе всех подсистем

СРОК ЛИЦЕНЗИРОВАНИЯ

- 1 год / 2 года / 3 года
- Продление лицензии возможно на 1 год

** рассчитывается индивидуально*

РАСШИРЕНИЕ ЛИЦЕНЗИИ

Для расширения объема лицензии (увеличение EPS) или уровня поддержки (SLA «Стандарт» и «Премиум») приобретается новая лицензия

КОНКУРЕНТНЫЙ ПЕРЕХОД

При использовании аналогичного решения возможен конкурентный переход. В данном случае предоставляется скидка до 70% от цен действующего прайс-листа (GPL) до конца второго квартала 2026 года

Как познакомиться с решением

SOLAR

ОНЛАЙН-ДЕМОНСТРАЦИЯ

Демонстрация работы Solar SIEM техническим пресейл-инженером

Условия:

- Демонстрация проводится в удобное для клиента время
- Инженер Solar SIEM отвечает на вопросы в ходе демонстрации
- Есть возможность подробно разобрать заинтересовавшие функции и модули

ПОДГОТОВКА К ПИЛОТНОМУ ТЕСТИРОВАНИЮ

Согласование технической части пилотного тестирования

Условия:

- Заполнение опросного листа для оценки инфраструктуры
- Определение целей и задач пилотного проекта
- Подготовка инфраструктуры к развертыванию
- Активная поддержка «Солара» на этапе подготовки

ПИЛОТНОЕ ТЕСТИРОВАНИЕ

Опытная эксплуатация в инфраструктуре заказчика

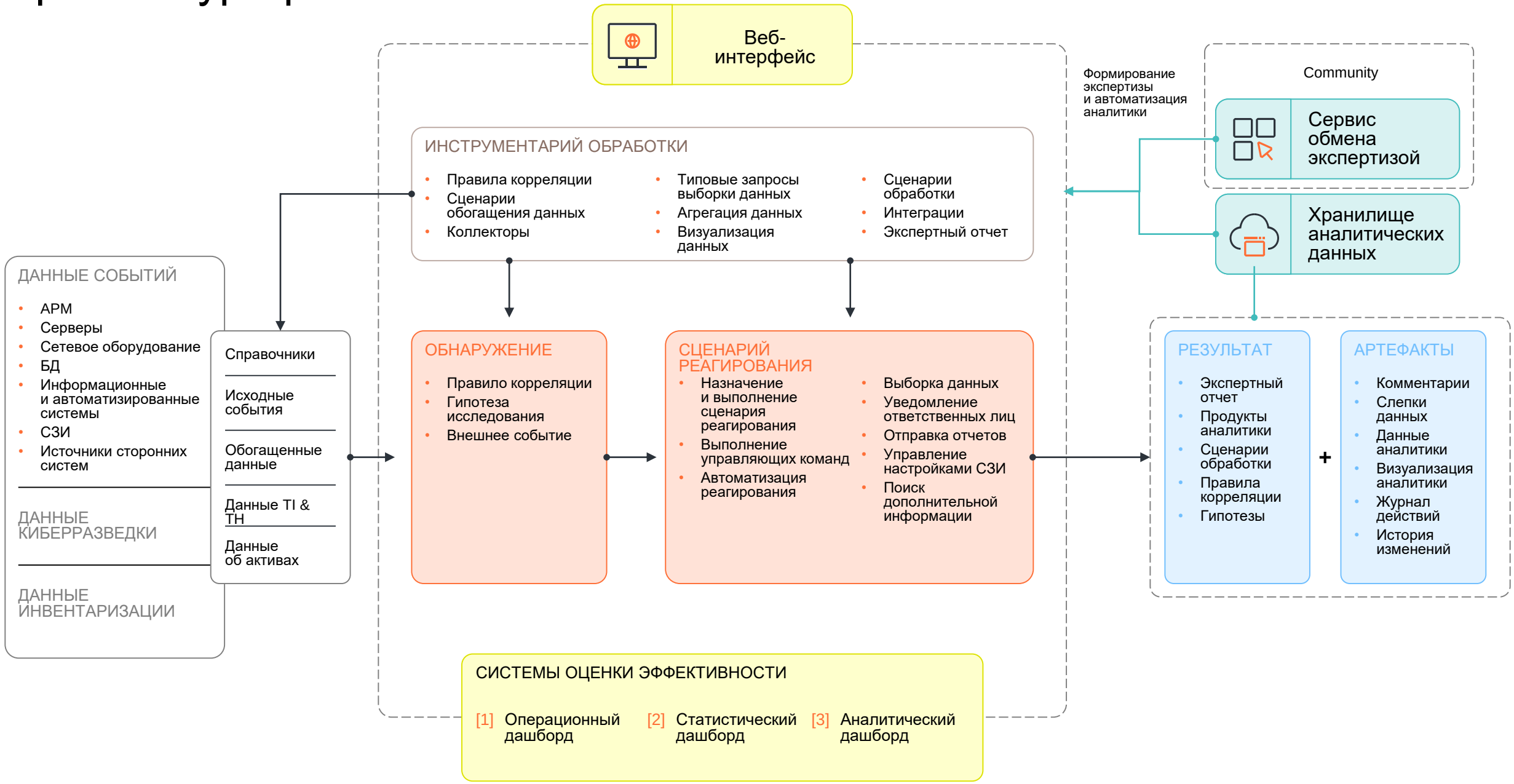
Условия:

- Поддержка в развертывании и настройке
- Вводное обучение по работе с Solar SIEM
- Выделенный пресейл-инженер на весь период пилотного тестирования
- Формирование итогового отчета
- Интеграция задач заказчика в план развития продукта

SOLAR

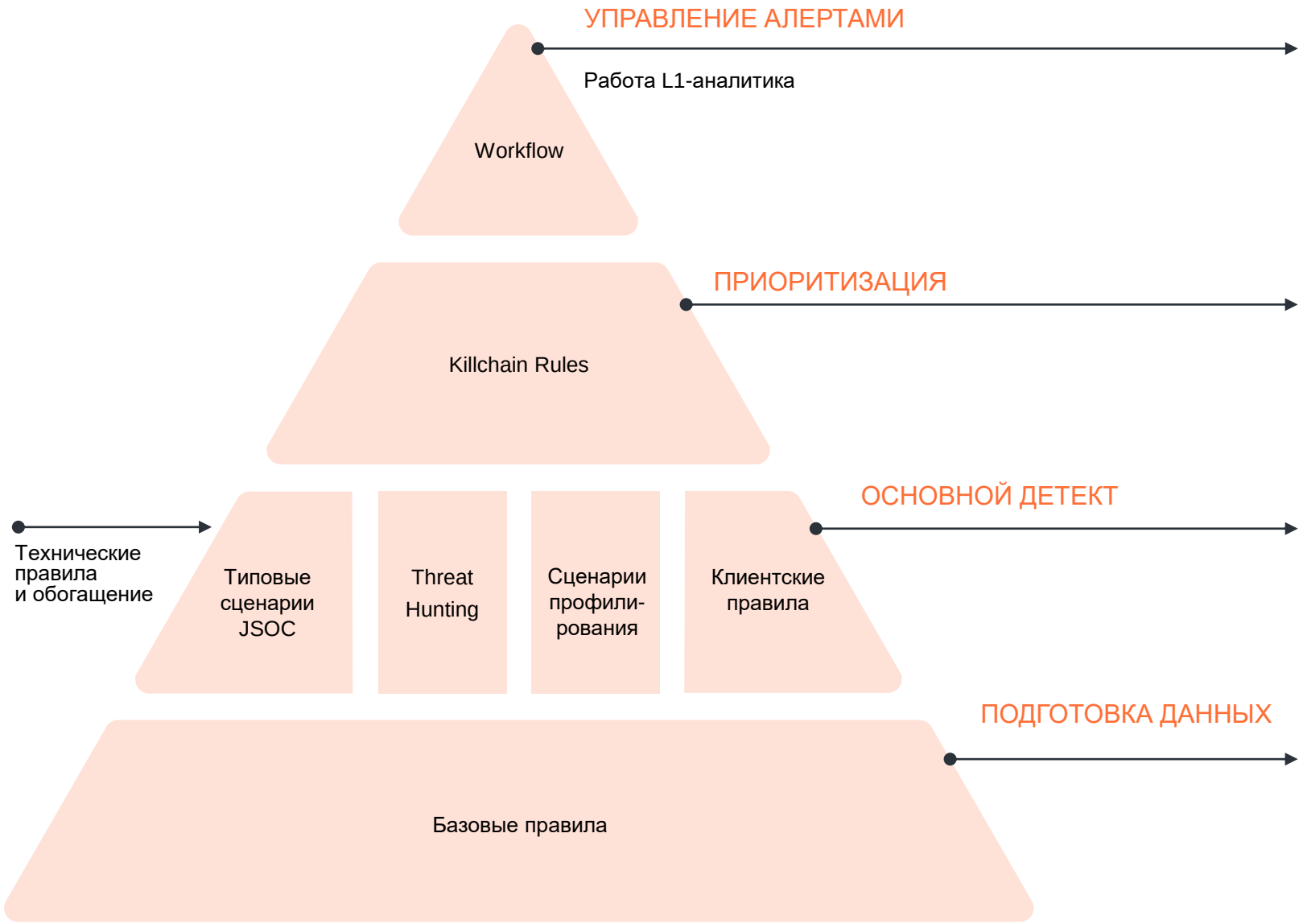
КОНЦЕПТУАЛЬНАЯ АРХИТЕКТУРА SOLAR SIEM

Архитектура решения



Унификация логики выявления инцидентов

SOLAR



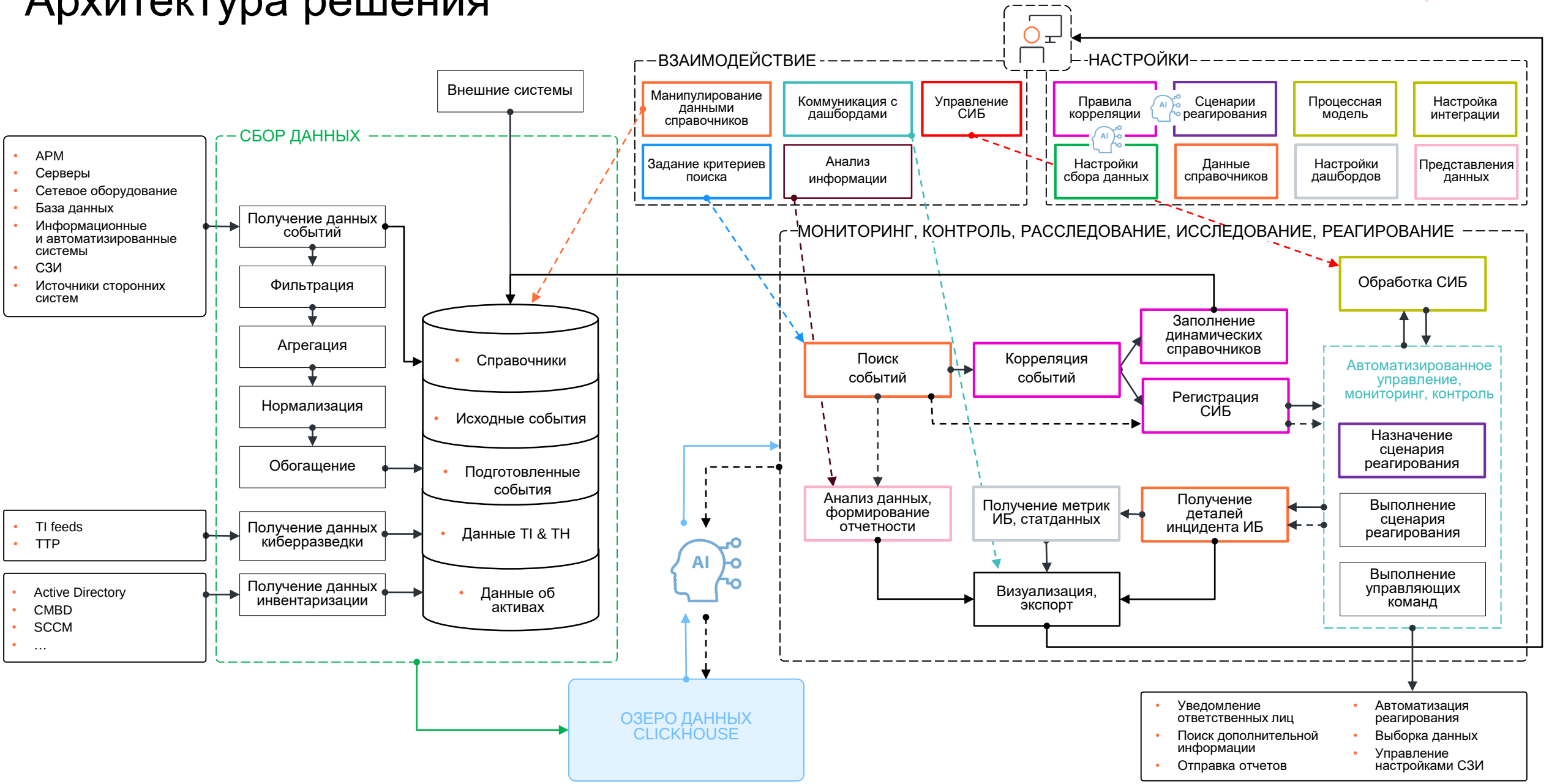
- Оповещения, создание кейсов, обработка информации
- Управление режимом работы правил
- Предотвращение флуда алертов

- Подсветка связанных алертов
- Повышение скорингов алертов
- Детектирование аномалий

- Правила не зависят от типа источников
- Добавление всего необходимого контекста
- Конфигурация под источник и исключения вне кода правил

- Добавление категоризации
- Добавление «пропущенной» информации
- Единая структура данных

Архитектура решения



Почему мы разбираемся в SIEM лучше других

SOLAR

2010

ПЕРВЫЕ ВНЕДРЕНИЯ SIEM

Изучение и внедрение ArcSight, Qradar, Symantec SIM NetForensics, Cisco MARS, Splunk

2012

ЗАПУСК SOLAR JSOC ВНУТРИ ОДНОЙ SIEM

- Накопление опыта на заказчиках с разными потребностями и условиями
- Инфраструктуры от 100 до 100k+ EPS
- Разработка единого подхода, позволяющего удовлетворить все запросы

2018

ПОЯВЛЕНИЕ MP SIEM В JSOC

- Опыт встраивания/замены SIEM на стороне заказчика
- Опыт масштабирования экспертизы
- Влияние опыта эксплуатации в JSOC на дорожную карту MP SIEM

2022

ПОЯВЛЕНИЕ KUMA В JSOC

- Внедрить новый SIEM на стороне заказчика — запросто!
- Прямое влияние опыта эксплуатации в JSOC на дорожную карту KUMA
- Третьего SIEM в JSOC не будет!

2025

SOLAR SIEM

- Максимально возможное соответствие современным требованиям к мониторингу и реагированию
- Объединение с «Гефест Технолоджиз»

SOLAR

ДОПОЛНИТЕЛЬНЫЕ УСЛУГИ

Личный кабинет ИБ для продуктов и сервисов

SOLAR

ЭТО ЕДИНАЯ ТОЧКА ВХОДА КЛИЕНТА В ЭКОСИСТЕМУ ПРОДУКТОВ И СЕРВИСОВ SOLAR, КОТОРАЯ ПОЗВОЛЯЕТ:

[01]

Просматривать контрактную информацию и сроки действия лицензии

[02]

Ознакомиться с документацией по продукту

[03]

Изучить инструкции конечных пользователей / администраторов

[04]

Узнать параметры подключенной технической поддержки

[05]

Получать актуальные анонсы обучающих вебинаров, конференций и воркшопов

[06]

Создавать обращения в техническую поддержку

[07]

Скачать лицензию

SOLAR

Оцените уникальность Solar SIEM на бесплатном пилотном тестировании

+7 (499) 755-07-70
info@rt-solar.ru

Центральный офис.
125009, Москва,
Никитский переулок, 7с1